PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

PUC- SP

RENAN AZEVEDO LEONESSA FERREIRA

O PAPEL DA VÍTIMA NOS CRIMES INFORMÁTICOS:

CONTRIBUIÇÕES DA VITIMODOGMÁTICA E DO FUNCIONALISMO PENAL EM BENS JURÍDICOS DISPONÍVEIS

São Paulo

2022

RENAN AZEVEDO LEONESSA FERREIRA

O PAPEL DA VÍTIMA NOS CRIMES INFORMÁTICOS:
CONTRIBUIÇÕES DA VITIMODOGMÁTICA E DO FUNCIONALISMO PENAL EM BENS JURÍDICOS DISPONÍVEIS

Dissertação de mestrado, como requisito parcial para obtenção do título de mestre em Direito Penal, sob a orientação do Prof. Dr. Guilherme de Souza Nucci.
Núcleo de pesquisa em Direito Penal.

São Paulo
2022

FICHA CATALOGRÁFICA

Ferreira, Renan Azevedo Leonessa.

O papel da vítima nos crimes informáticos: contribuições da vitimodogmática e do funcionalismo penal em bens jurídicos disponíveis / Renan Azevedo Leonessa Ferreira. -- São Paulo, 2022.

217 p.; 15 cm.

Orientador: Prof. Dr. Guilherme de Souza Nucci.

Dissertação (Mestrado) -- Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós Graduados em Direito.

1. Crimes Informáticos. 2. Vitimodogmática. 3. Funcionalismo penal. 4. Bem jurídico disponível.

I. Nucci, Guilherme de Souza. II. Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós Graduados em Direito. III. Título.

RENAN AZEVEDO LEONESSA FERREIRA

O PAPEL DA VÍTIMA NOS CRIMES INFORMÁTICOS:
CONTRIBUIÇÕES DA VITIMODOGMÁTICA E DO FUNCIONALISMO PENAL EM BENS JURÍDICOS DISPONÍVEIS

Dissertação de mestrado, como requisito parcial para obtenção do título de mestre em Direito Penal, sob a orientação do Prof. Dr. Guilherme de Souza Nucci.
Núcleo de pesquisa em Direito Penal.

São Paulo, 03 de junho de 2022.

Banca examinadora:

_____
Prof. Dr. Guilherme de Souza Nucci

_____
Prof. Dr. Oswaldo Henrique Duek Marques

_____
Prof. Dr. Jamil Chaim Alves

Dedico este trabalho aos meus pais e à Juliana, que sempre me acompanham em minha trajetória pessoal e acadêmica.

AGRADECIMENTOS

Agradeço a meu orientador, professor Guilherme Nucci, por acreditar em meu trabalho e não medir esforços em me auxiliar neste período desfiador. Pelas valiosas contribuições e apoio imensurável em uma orientação integralmente a distância.

Agradeço aos professores Oswaldo Duek, Cláudio Langroiva e Antonio da Ponte pelas aguçadas disciplinas na pós-graduação, que abriram novas perspectivas para esta pesquisa.

Agradeço ao professor Christiano Jorge pelas relevantes observações para o aprimoramento do trabalho.

Agradeço a meu tio Cláudio, que sempre me incentivou e auxiliou desde o início de minha trajetória acadêmica.

Agradeço a meus amigos Matheus, Pedro e Josianne, por todo o suporte em meus estudos no mestrado.

Agradeço à Pontifícia Universidade Católica de São Paulo e, em especial, ao setor de pós-graduação em direito, pela oportunidade acadêmica e pelo eficaz auxílio virtual neste período.

"We" could still be we, the people, you and me. Building on our individual responsibility, as informed human beings, conscious of our duties, confident in our projects. Indeed, only if you and I, and all the others, are responsible for what we do, and feel responsible for what happens around us, can our society control and guide this unprecedented technological creativity.

CASTELLS, Manuel. *The Internet Galaxy: reflections on the lnternet, business and society.* New York: Oxford University Press, 2001, p. 282.

RESUMO

FERREIRA, Renan Azevedo Leonessa. *O papel da vítima nos crimes informáticos:* contribuições da vitimodogmática e do funcionalismo penal em bens jurídicos disponíveis

Com o avanço tecnológico e incremento do uso cotidiano de dispositivos informáticos, também se potencializaram os delitos praticados no ambiente virtual, sendo imprescindível certa contribuição da vítima para a consumação de condutas lesivas a bens jurídicos disponíveis. Esta pesquisa tem por objetivo analisar a possível repercussão do comportamento negligente ou desidioso dos usuários sobre a responsabilidade penal do autor em crimes informáticos próprios (ligados à proteção de dados pessoais) e impróprios relacionados a bens jurídicos disponíveis (notadamente, o patrimônio), à luz das contribuições vitimodogmáticas e funcionalistas, tendo por base o valor constitucional do livre desenvolvimento da personalidade. Para tanto, adota-se o método dedutivo de pesquisa para o levantamento teórico e bibliográfico, enquanto é empregado o método dialético para a aplicação dos elementos criminológicos e político-criminais na seara informática sobre a dogmática penal. Ao longo do trabalho, conclui-se pela viabilidade da mitigação da responsabilidade penal do autor, ou mesmo atipicidade de sua conduta, à luz dos postulados vitimodogmáticos e do funcionalismo moderado, em prestígio à autorresponsabilidade dos usuários na sociedade de risco, valor dotado de cariz constitucional. Conforme se depreende das teorias criminológicas emergentes para o ambiente informático, isso dependerá de uma análise casuística com base na desídia de atuação da vítima no ambiente virtual, bem como tendo em vista as características próprias do usuário, mormente seu grau de domínio tecnológico.

Palavras-chave: Crimes informáticos. Vitimodogmática. Funcionalismo Penal. Bem jurídico disponível. Política Criminal.

ZUSAMMENFASSUNG

FERREIRA, Renan Azevedo Leonessa. *Die Rolle des Opfers bei Computerkriminalität*: Beiträge von Viktimodogmatik und strachrechtlichem Funktionalismus bezüglich verfügbarer Rechtsgüter.

Mit dem technologischen Fortschritt und der zuhnemenden täglichen Nutzung von Computergeräten haben auch die in der virtuellen Umgebung begangenen Straftaten zugenommen, wobei ein gewisser Beitrag des Opfers für die Volziehung eines verfügbaren Rechtsgüter schädigenden Verhaltens wesentlich ist. Das Ziel dieser Forschung besteht auf dem möglichen Einfluss von fahrlässigen oder leichtfertigen Verhalten der Benutzern auf die strafrechtliche verantworlichkeit des Täters angesichts angemessener Computerkriminalität (bezogen auf den Schutz personanbezogener Daten) und unangemesser Computercriminalität in Zusammenhang mit verfügbaren Rechtsgütern (insbesondere mit dem Eigentum), im Licht von Viktimodogmatik und Fuktionalismus, basierend auf dem verfassungsmässigen Wert der freien Entwicklung der Persönlichkeit. Dazu wird für die theoretische und bibliographische Forschung die deduktive Forschungsmethode angewandt, während die dialektische Methode für die Anwendung kriminologischer und kriminellpolitischer Elemente im Computerstraftaten zur Strafdogmatik verwendet wird. Bei der Forschung wird daraus schliessen, dass eine Abmilderung der strafrechtlichen Verantworlichkeit des Täters, oder sogar keine Erfüllung von Tatbestand, möglich ist angesichts der Eigenverantwortung der Benutzer in der Risikogesellschaft, ein Wert von verfassungsrechtlichem Rang. Wie aus neuen kriminologischen Theorien für die Computerumgebung hervorgeht, hängt dies von einer Einzellfalanalyse ab, die auf der Fahrlässigkeit des Opfers beim Handeln sowie auf die eigenen Eigenschaften des benutzers beruht, hauptsächlisch auf die Beherrschung von Technologien.

Schlüsselwörter: Computerstraftaten. Viktimodogmatik. Strafrechtlicher Funktionalismus. Verfügbares Rechtsgut. Kriminellpolitik.

LISTA DE ABREVIATURAS E SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ARPA	Advanced Research Projects Agency
CPU	Central Processing Unit
DDoS	Distributed Denial of Servive
DoS	Denial of Service
ENISA	European Agency for Network and Information Security Agency
HD	Harddrive
HTTPS	Hypertext Transfer Protocol Secure
iOS	iPhone Operating System
IP	Internet Protocol
LGPD	Lei Geral de Proteção de Dados
ONG	Organização Não Governamental
RAT	Routine Activities Theory
ROBERT	Risktaking Online Behaviour Empowerment Through Research and Training
SCP	Situational Crime Prevention
SQL	Structured Query Language
TOR	The Onion Router
URL	Uniform Resource Locator

SUMÁRIO

INTRODUÇÃO

O tema da presente pesquisa diz respeito ao papel da vítima na conformação da conduta delitiva diante de crimes informáticos próprios e impróprios relacionados a bens jurídicos disponíveis. Parte-se do pressuposto constitucional do livre desenvolvimento da personalidade, como fruto da dignidade humana, a conferir um caráter ativo no exercício da autonomia dos usuários no ambiente informático. Busca-se analisar o surgimento de um novo bem jurídico na seara virtual, bem como compreender novas formas de lesão ao bem jurídico patrimônio, tradicionalmente tutelado no ordenamento pátrio. Fincadas essas balizas, recorre-se à criminologia e à política criminal para a compreensão da função central desempenhada pelos usuários na seara dos delitos informáticos, perquirindo-se acerca de sua repercussão na responsabilidade penal do autor sob a ótica vitimodogmática e sob o funcionalismo penal.

Dentro dessa temática, o objeto da pesquisa consiste em analisar em que medida o comportamento negligente ou desidioso dos usuários é apto a repercutir sobre a responsabilidade penal do autor diante de crimes informáticos próprios e impróprios atinentes a bens jurídicos disponíveis, à luz das contribuições vitimodogmáticas e funcionalistas lastreadas na projeção ativa do valor constitucional do livre desenvolvimento do indivíduo.

A relevância do tema, de início, se justifica pela multiplicação da prática de crimes informáticos, com frequentes e relevantes violações a dispositivos informáticos, dados pessoais e patrimônio, concomitantemente à necessidade de assunção de papel protagonista e autônomo pelos usuários nesse ambiente.

Com efeito, o impulso tecnológico das últimas décadas viabilizou a realização de inúmeras atividades à distância, circunstâncias inclusive catalisadas pela pandemia de COVID-19 nos anos de 2020 e 2021. Atualmente, inúmeras atividades cotidianas podem ser efetuadas por meio de um dispositivo informático: compras, lazer, trabalho (por meio do *home office*), transações financeiras (*Internet Banking*). A sociedade, assim, torna-se interconectada, fazendo jus à denominação proposta por Manuel Castells: é a sociedade em rede.

Do outro lado da moeda, com o avanço tecnológico também há forte impulsionamento de práticas delitivas nesse novo ambiente virtual, que se torna uma das vertentes da sociedade de risco, sendo certo que fatores como anonimato, onipresença e o caráter individualista do uso da Internet são explorados pelos agentes. No mais, em se tratando de bens jurídicos disponíveis – para os fins propostos, a autodeterminação informática e o patrimônio –, verifica-se que com

frequência é pressuposta alguma conduta ou omissão culposa do usuário[1]. Dessa forma, o elo mais frágil nesses delitos consiste justamente no usuário, que se torna decisivo para o sucesso da empreitada delitiva.

Esse elo frágil, contudo, diz respeito a um indivíduo dotado de autonomia e capaz de se autodeterminar em sociedade. Com efeito, quando se está ciente dos riscos de uma exposição ao ambiente virtual, o usuário não pode ser vislumbrado como mero sujeito passivo da conduta delitiva – conforme se apregoa uma visão penal paternalista –, mas sim como ser humano racional, em prol da manifestação ativa de seu livre desenvolvimento da personalidade, valor constitucional lastreado na dignidade da pessoa humana.

Não se trata de responsabilizar a vítima pelo fenômeno delitivo, mas sim de reconhecer seu protagonismo em sua gênese, em um movimento de resgate de sua dignidade e autonomia já iniciado desde o fim da Segunda Guerra Mundial. Logo, a compreensão do usuário no ambiente informático perpassa por necessários estudos criminológicos e vitimológicos, que reinserem a vítima na gênese do fenômeno delitivo.

Voltando-se à ciência jurídico-penal, estudos vitimodogmáticos ressaltam a importância de se compreender a repercussão que a conduta da vítima possui sobre a prevenção delitiva e a adequada análise da responsabilidade penal do agente, o que se torna de magna pertinência para a estudo de crimes informáticos alusivos a bens jurídicos disponíveis.

Sob uma ótica sistematizadora e inserido na atual sociedade de risco informática, adquire relevância também o funcionalismo penal, particularmente sob sua vertente moderada concebida por Claus Roxin, que postula uma integração entre critérios político-criminais e a dogmática penal. Destarte, convém analisar o comportamento da vítima frente aos delitos informáticos sob o viés da teoria da imputação objetiva, com destaque para a autocolocação em risco, cuja necessidade de investigação já foi aventada por doutrinadores como Damásio de Jesus, Marcelo Crespo e Spencer Sydow.

A presente pesquisa torna-se relevante à medida que, partindo-se da autonomia humana como fator chave para o livre desenvolvimento da personalidade, recorre a critérios criminológicos e político-criminais, com enfoque sobre a vítima dos delitos informáticos, a fim de propor elementos ensejadores da prevenção desses crimes. Direciona-se, assim, na contramão do legislador penal pátrio, que recorre a uma pulverização de tipos penais e

[1] Logo, não se está a falar de acordo ou consentimento do titular do bem jurídico tutelado, que pressupõe plena anuência com o resultado alcançado. A título exemplificativo, cite-se um usuário que efetua o *download* de um arquivo malicioso, ou mesmo transfere valores após encontrar um anúncio de produto vendido por preço inferior ao de mercado.

incremento penal sem embasamento empírico, em inócuo movimento punitivista, atualmente consubstanciado pela Lei n. 14.155/2021. Entende-se, dessa forma, que em prol dos princípios da culpabilidade e intervenção mínima deve-se privilegiar a autorresponsabilidade do usuário médio diante de bens jurídicos disponíveis, mitigando-se a responsabilidade penal em prol de concreta e efetiva prevenção delitiva na sociedade de risco informática.

Para a redação do trabalho, parte-se de uma associação entre os métodos dedutivo e dialético. Mediante a análise das referências bibliográficas, de artigos e publicações referentes ao tema, elaborar-se-á uma cadeia de raciocínio particularmente na análise dos aspectos gerais dos fundamentos constitucionais e penais delitos informáticos, da vitimodogmática e do funcionalismo. Assim, busca-se elaborar sínteses das leituras acrescidas de comentários e visões críticas, considerando os objetivos formulados.

Outrossim, dada a insuficiência da aplicação desse método, a estratégia dialética será predominante no desenvolvimento e na consecução dos objetivos da pesquisa. Isso se deve ao fato da impossibilidade de compreender a realidade sob uma ótica objetiva, de modo que se faz necessário associar o atual contexto da sociedade a teorias criminológicas empíricas. Assim, levar-se-á em conta a inter-relação entre os fatos e fenômenos na realidade sob uma ótica de mudança – na atual sociedade de risco –, de modo a extrair possíveis contradições e crise do paradigma atual do Direito Penal no que tange à participação da vítima nos delitos informáticos e possíveis medidas preventivas a ser adotadas. A precípua expressão do método dialético se manifestará na análise de subsunção entre as propostas vitimodogmáticas e funcionalistas à luz das teorias criminológicas emergentes quanto aos delitos informáticos.

No mais, deve-se ressaltar que a elaboração da presente dissertação integralmente em período pandêmico dificultou o acesso a livros e bibliotecas físicas, recorrendo-se majoritariamente ao acesso on-line ou à aquisição virtual de obras. De qualquer modo, não se vislumbra prejuízo científico ao resultado obtido, inclusive em razão da facilidade de acesso a obras no ambiente informático.

Para atingir o escopo da presente pesquisa, serão traçadas inicialmente as bases constitucionais da tutela de dados pessoais, com destaque ao ambiente virtual, remetendo-se ao livre desenvolvimento do indivíduo como fundamento da autonomia dos usuários quanto à sua exposição aos riscos informáticos. A candência do tema é reforçada pelo reconhecimento da proteção a dados pessoais como direito fundamental explícito na Constituição Federal, com o advento da Emenda Constitucional n. 115/2022. Sob a ótica penal, procede-se ao reconhecimento de um novo bem jurídico na seara virtual, intrinsecamente ligado à proteção de dados pessoais, cuja fundamentação decorre da Constituição Federal. Com isso, viabiliza-se

uma análise dos principais crimes informáticos próprios e impróprios alusivos a bens jurídicos disponíveis, com destaque para a autodeterminação informática e o patrimônio.

Fincadas as bases constitucionais, torna-se de magna relevância recorrer a promissoras propostas criminológicas emergentes na seara informática como forma de adaptação da Criminologia ao ambiente virtual, mormente reconhecendo-se o papel central desempenhado pelo usuário - sobre quem recai essencialmente a tomada de decisões cotidianas. A partir da teoria das atividades rotineiras e da prevenção situacional do crime, são traçados comportamentos diligentes a ser adotados pelos usuários como medidas de prevenção delitiva. Sob o viés vitimológico, efetua-se uma classificação das vítimas informáticas, analisando-se sua vulnerabilidade, com destaque para a ignorância tecnológica – recomendando-se sua paulatina superação por meio do acesso digital a todos e de educação digital.

Pavimentados os aspectos criminológicos no ambiente informático, delineiam-se dois caminhos paralelos e não excludentes. Por um lado, aglutinam-se as conclusões sob a ótica vitimodogmática, analisando-se as principais correntes e possíveis repercussões penais sobre a responsabilização penal o autor. No contexto virtual, em que a conduta de cada usuário ganha relevo, a vitimodogmática emerge como eficaz ferramente de reinserção do papel da vítima na seara dogmática penal. Por outro lado, promove-se uma análise à luz do funcionalismo penal, com destaque a sua corrente moderada, o que se mostra de premente necessidade na dita sociedade de risco, que tem uma de suas principais manifestações nos crimes informáticos.
Assim, torna-se possível estabelecer diretrizes acerca da repercussão do comportamento dos usuários virtuais sobre a conduta delitiva perante bens disponíveis, reforçando-se a autorresponsabilidade como forma de corroborar uma política-criminal voltada à manutenção dos valores do Estado Democrático de Direito e à prevenção delitiva, de modo a refrear as tendências punitivistas atécnicas já desencadeadas nesse novo ambiente.

1. FUNDAMENTOS CONSTITUCIONAIS E JURÍDICO-PENAIS DA TUTELA DE DADOS PESSOAIS

O avanço cronológico da história da humanidade indica o surgimento de novos interesses dignos de tutela jurídica. Na sociedade em rede e de risco atual não são raras as condutas potencialmente lesivas a interesses individuais e coletivos dos usuários de dispositivos informáticos. Por outro lado, o ambiente informático se torna um novo polo de desenvolvimento do ser humano e de suas atividades cotidianas. Por essa razão, neste Capítulo recorre-se aos contornos de um novo direito fundamental, a partir de um feixe de valores constitucionais que converge para a tutela de dados pessoais (plasmada como a autodeterminação informativa, conforme reconhecido pelo Supremo Tribunal Federal em 2020, e consolidada como direito fundamental explícito em 2022), decorrente da dignidade da pessoa humana como fundamento para o livre desenvolvimento da personalidade. Na sociedade de risco e em rede, confere-se particular destaque a uma vertente positiva da tutela jurídica dos usuários no ambiente virtual, em reconhecimento a sua autodeterminação informática.

1.1. Desenvolvimento de um novo direito fundamental e sua construção constitucional

Notadamente após graves violações a direitos humanos praticadas na Segunda Guerra Mundial, o princípio da dignidade humana emergiu nas Constituições estatais, impulsionado pela Declaração dos Direitos Humanos das Nações Unidas.[2] No ordenamento pátrio, a dignidade humana é considerada fundamento da República, plasmada em seu artigo 1º, inciso III. Sarlet conceitua a dignidade humana como:

> Qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existentes mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos.[3]

Apesar de seu elevado grau de abstração, a importância e eficácia da dignidade humana decorrem de sua natureza reitora do ordenamento, tornando-se uma norma-princípio apta a

[2] Artigo 1º: Todos os seres humanos nascem livres e iguais em dignidade e direitos. São dotados de razão e consciência e devem agir em relação uns aos outros com espírito de fraternidade.
[3] SARLET, Ingo Wolfgang. *Dignidade da Pessoa Humana e Direitos Fundamentais na Constiuição Federal de 1988*. 2. ed. Porto Alegre: Livraria do Advogado, 2002, p. 62.

fornecer um padrão de interpretação das demais normas de direitos fundamentais, vedando-se hipóteses de desrespeito à própria humanidade do indivíduo.[4]

O deslocamento do eixo jurídico colocou o ser humano em sua centralidade, o que levou a uma despatrimonialização da esfera civil[5] e, na esfera penal, conduz a uma maior atenção à vítima, ao sujeito em si, em detrimento de simples monetização de prejuízos. Com isso, valoriza-se o livre desenvolvimento do indivíduo, quem se torna apto a tomar as próprias decisões como ser dotado de dignidade e racionalidade. Seus valores, aliás, encontram-se plasmados no artigo 29 da Declaração dos Direitos Humanos das Nações Unidas.[6]

Nesse contexto, foram impulsionados e valorizados os direitos da personalidade, sendo esta compreendida como o conjunto de traços distintivos de um indivíduo. Como aponta Bittar:

> Consideram-se da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, o segredo, o respeito, a honra, a intelectualidade e outros tantos.[7]

Muito embora a concepção de direitos da personalidade tenha em geral viés civilístico, eles denotam simplesmente a ótica constitucional de direitos fundamentais pessoais, emergindo como proteção da esfera nuclear individual do ser humano, em sua relação intrínseca com a dignidade.[8] Busca-se tutelar, com isso, o livre desenvolvimento da personalidade do indivíduo, manifestando-se como uma proteção abrangente a ingerências, ainda que não expressas na Constituição Federal, mas dela decorrentes.

Originalmente, com o surgimento do Constitucionalismo Moderno, a proteção da personalidade residia essencialmente em refrear incursões estatais sobre a esfera de autonomia do indivíduo. Contudo, com o resgate do princípio da dignidade humana após a Segunda Guerra Mundial, adquire um prisma mais amplo, que abrange tanto a proteção em face de particulares,

---

[4] MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, pp. 813-815.

[5] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 95.

[6] 1.Todo ser humano tem deveres para com a comunidade, na qual o livre e pleno desenvolvimento de sua personalidade é possível. 2. No exercício de seus direitos e liberdades, todo ser humano estará sujeito apenas às limitações determinadas pela lei, exclusivamente com o fim de assegurar o devido reconhecimento e respeito dos direitos e liberdades de outrem e de satisfazer as justas exigências da moral, da ordem pública e do bem-estar de uma sociedade democrática. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 29 set. 2021.

[7] BITTAR, Carlos Alberto. *Os direitos da personalidade*. São Paulo: Saraiva, 2015, p. 26.

[8] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, p. 455.

como também um aspecto ativo, como forma de exercício da própria autonomia, que permite a manifestação da personalidade de cada indivíduo. Como apontam Sarlet, Marinoni e Mitidiero:

> O direito de personalidade, embora tenha por objeto a proteção contra intervenções na esfera pessoal, é também um direito de liberdade, no sentido de um direito de qualquer pessoa a não ser impedida de desenvolver sua própria personalidade e de se determinar de acordo com suas opções. [9]

Muitos ordenamentos fazem menção expressa ao livre desenvolvimento da personalidade, como as Constituições da Alemanha, Espanha e Portugal. No Brasil, muito embora não conste sua menção do ordenamento constitucional, seus preceitos são extraídos diretamente da dignidade da pessoa humana (como fundamento da República Federativa do Brasil, conforme artigo 1º, inciso III) e do direito individual à liberdade (artigo 5º, *caput*), que pressupõem o respeito à autonomia do indivíduo.

O livre desenvolvimento da personalidade não apresenta mero caráter complementar aos demais direitos individuais – e até mesmo sociais –, mas representa um caráter independente e de efetiva conformação dos demais direitos como forma de resguardar a liberdade de ação individual em sua integralidade: sobressai tanto o aspecto obrigacional estatal – de refrear ingerências sobre certo direito ou de promover políticas públicas para resguardá-lo – como a vertente positiva de atuação do indivíduo como ser apto a tomar as próprias decisões.[10]

Trata-se, assim, de diferentes modos de desenvolvimento do titular: determinação autônoma de seu destino sem intervenção estatal ou de particulares (autodeterminação), escolha da forma de apresentação ao público (autoexposição) e eventualmente se apartar do mundo externo (autoconservação). Protege-se, assim, todos os prismas da liberdade de ação em determinados setores que historicamente sofrem maior intervenção pelo poder público.[11_12]

Quanto ao ponto, a dignidade humana exercerá uma função dúplice: enquanto fundamenta a renúncia concreta a determinado direito individual (nunca ao direito em abstrato), também impõe limites quando se está diante de valores caros ao ordenamento, como a vida, vedação à tortura e ao trabalho escravo.[13] Por essa razão, conforme aponta Martins, devem ser

---

[9] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, p. 460.
[10] Ibidem, p. 460-462. Trata-se, com isso, de "preservar as potencialidades de cada direito em espécie".
[11] MARTINS, Leonardo (org). *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Trad. Beatriz Hennig; Leonardo Martins; Mariana Bigelli de Carvalho; Tereza Maria de Castro e Vivianne Geraldes Ferreira. Montevidéu: Konrad Adenauer, 2005, pp. 190-193.
[12] Na esfera penal, essa intervenção se manifesta frequentemente por meio do paternalismo, com a tutela de condutas contrariamente ao interesse demonstrado pelo titular do bem jurídico no caso concreto.
[13] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, pp. 464-465.

considerados fundamentais todos os direitos que materializem algum prisma da dignidade da pessoa humana.[14] Como se vê, portanto, nem todos os direitos fundamentais são atrelados à personalidade, porém todos os direitos da personalidade são fundamentais.

Posto que decorrente da própria dignidade humana – que ressalta o valor intrínseco do ser humano – destaca-se o caráter extrapatrimonial dos direitos da personalidade, de modo que seu exercício não é economicamente apreciável. Trata-se de um bem ou interesse intrinsecamente relacionado à subjetividade de cada indivíduo, de modo que os reflexos patrimoniais não são determinantes para sua análise.[15]

Como um dos prismas irradiadores da dignidade humana, surge a progressiva pertinência de proteção de dados pessoais, alçada ao patamar de direito da personalidade e direito fundamental porquanto diz respeito à esfera pessoal do indivíduo para seu desenvolvimento em sociedade. Deve-se pontuar que a proteção de dados pessoais, inclusive no ambiente digital, já possuía *status* de direito fundamental implícito no ordenamento pátrio. Seu reconhecimento expresso, no entanto, ocorreu com o advento da Emenda Constitucional n. 115/2022, que acrescentou o inciso LXXIX ao artigo 5º da Carta Maior.[16]

Tradicionalmente, a noção de dados pessoais diz respeito a informações de caráter personalíssimo que permitam identificação ou determinação, ainda que indireta, de seu titular.[17] De particular destaque são os dados sensíveis, que abrangem informações de particular vulnerabilidade, posto que aptas a fomentar discriminação, tais como origem étnica, convicções políticas, religiosas, preferências sexuais.[18]

Na compreensão de Bioni, sob o conceito de dados pessoais não são abarcadas apenas informações reveladoras ou aptas revelar a identidade do sujeito, mas também qualquer

---

[14] MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, p. 792.

[15] Referido raciocínio se mostra de particular relevância para a posterior análise conjugada dos delitos informáticos atinentes a bens jurídico patrimônio, em que não necessariamente haverá conformação de conduta delitiva diante de um ato que implique uma redução patrimonial de seu titular.

[16] Artigo 5º, LXXIX: é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[17] Nesse sentido, a LGPD, em seu artigo Art. 5º: Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

[18] SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro. In: De Lima, Cíntia Rosa Pereira (coord). *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020, p. 19. Assim restou plasmado o artigo 5º, inciso II, da LGPD (BRASIL, 2018): II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

conteúdo que confira impacto ao titular do dado.[19–20] Afinal, conforme o entendimento de Bioni: "[h]oje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses signos identificadores do cidadão. Isso acaba por justificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade.".[21]

Nesse contexto, como aponta Martins, a proteção a dados pessoais visa a tutelar a intimidade, privacidade, honra e imagem dos usuários, valores que encontram seu fundamento no artigo 5º, inciso X, da Constituição Federal, aliados ao artigo 2º, inciso IV, da Lei Geral de Proteção de Dados (LGPD).[22] Por não corresponder a direitos fundamentais já individualmente elencados na Carta Maior, com razão o poder constituinte derivado ao reconhecê-lo explicitamente como direito fundamental autônomo.

Com efeito, a proteção a dados pessoais diz respeito ao resguardo da honra em seus aspectos objetivo (imagem projetada pela sociedade acerca do indivíduo) e subjetivo (imagem que a própria pessoa possui de si), à imagem social (apresentação perante a sociedade da pessoa física ou jurídica), à imagem-retrato (representação da pessoa em desenhos, pinturas, fotografias) e à imagem autoral (referente à presença do autor em obras coletivas).[23] De fato, a obtenção de dados pessoais por terceiros e sua difusão em larga escala é apta a macular todos esses aspectos da projeção do indivíduo sobre a sociedade, bem como perante si mesmo. Como manifestação dos direitos da personalidade, os dados revelam uma projeção do próprio indivíduo, bem como influem sobre sua inter-relação com os demais, de modo que sua proteção se torna essencial para o livre desenvolvimento da personalidade de seu titular.[24]

---

[19] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 113. Por essa razão, aliás, a LGPD confere inclusive proteção a dados anonimizados empregados no rastreamento de perfis comportamentais (artigo 12, §2º).

[20] De fato, conforme aponta Sarlet, há um conglomerado de informações que possuem valor político e econômico, posto que podem ser utilizados como mecanismos de controle social – como a indução a aquisição de determinados produtos -, algo fomentado com o emprego de algoritmos implementados por inteligência artificial. (SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro. In: De Lima, Cíntia Rosa Pereira (coord). *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020, p. 20). Atualmente, assim, o emprego da informação torna-se central sob as perspectivas política e econômica, no termo alcunhado por Castells como informacionalismo. Segundo esse autor: "no informacionalismo, as tecnologias assumem um papel de destaque em todos os segmentos sociais, permitindo o entendimento da nova estrutura social – sociedade em rede – e consequentemente, de uma nova economia, na qual a tecnologia da informação é considerada uma ferramenta indispensável na manipulação da informação e construção do conhecimento pelos indivíduos." (CASTELLS, Manuel. *A Era da Informação: economia, sociedade e cultura*. Vol. 3. São Paulo: Paz e Terra, 1999, p. 21).

[21] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 99.

[22] MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, p. 395.

[23] Ibidem, p. 395-396.

[24] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 118.

Ademais, de especial destaque é a tutela à vida privada e à intimidade. Aquela entende-se como todos os relacionamentos diários de um indivíduo, seja no trabalho, seja no estudo, ou em passeios. A intimidade, a seu turno, guarda relação com círculos mais próximos de relacionamento, de modo a consistir em um núcleo da vida privada.[25] Destarte, qualquer obtenção indevida de dados pessoais acerca do usuário diz respeito, ao menos, à violação à sua vida privada, bem como, frequentemente, a sua intimidade.

Deve-se observar, contudo, que a proteção de dados não se limita ao aspecto negativo do direito à privacidade, compreendido como o "right to be alone", vedando-se ingerências externas sobre a esfera particular do indivíduo. Projeta-se, ainda, em uma vertente positiva, como um espaço de desenvolvimento e construção do indivíduo, que se torna efetivo controlador e gerenciador de seus dados em prol da consecução de seus objetivos dispostos a serviço do desenvolvimento de sua personalidade.[26]

Destarte, verifica-se que o direito à proteção de dados pessoais transborda o já consagrado direito à privacidade, com vistas a se promover uma ampla observância ao livre desenvolvimento do indivíduo, lastreado na dignidade da pessoa humana. Esta é a posição precursora adotada por Stefano Rodotà ao conferir autonomia à proteção dos dados no bojo dos direitos à personalidade.[27] Por essa razão, partindo-se de uma ótica do indivíduo, emerge a necessidade de tutela geral à liberdade, compreendida como a possibilidade de autodeterminação do ser humano.[28] Logo, sua proteção também deriva diretamente do artigo 5º, inciso II, da Constituição Federal: "ninguém será obrigado a fazer ou deixar de fazer alguma coisa, senão em virtude de lei.".

Outro pilar constitucional, derivado do direito à liberdade, o artigo 5º, inciso XII, impõe a inviolabilidade do sigilo da correspondência, comunicações telegráficas, comunicações telefônicas e, notadamente, de dados. Na atualidade, verifica-se uma transferência da relevância da tutela, antes concentrada em comunicações telefônicas e telegráficas, para o resguardo de dados, o que engloba o envio de e-mails, mensagens por aplicativos, videoconferências e outros.[29] Por essa razão, a interceptação telefônica, telemática ou informática apenas poderá ser autorizada mediante decisão judicial (artigo 1º, *caput* e parágrafo único, da Lei n. 9.296/1996).

---

[25] MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, p. 396.
[26] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 126.
[27] Cf. RODOTÁ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014.
[28] Quanto à autodeterminação no ambiente informático, cf. NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 3, 4. ed. Rio de Janeiro, Forense, 2019.
[29] MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, p. 404

Não se pode olvidar também a garantia constitucional do Habeas Data, previsto no artigo 5º, inciso LXXII, a assegurar ao titular o acesso a informações constantes de bancos de dados de órgãos públicos, bem como sua retificação. Trata-se, com isso, de conferir ao titular controle sobre as informações que o Estado possui sobre si, permitindo-lhe, se o caso, eliminá-las ou retificá-las.

Por fim, de modo complementar a essa garantia constitucional, o artigo 19, do Pacto Internacional sobre Direitos Civis e Políticos, prevê a liberdade de informação, consistente no direito de "procurar, receber e difundir informações e ideias de qualquer natureza independentemente de considerações de fronteiras, verbalmente ou por escrito, de forma impressa ou artística, ou por qualquer meio de sua escolha". Convém ressaltar que, à luz do artigo 5º, §3º, da Constituição Federal, o direito à informação, previsto em tratado internacional ratificado pelo Brasil, foi erigido ao status de direito fundamental.

Como se vê, pode haver certa superposição desse direito fundamental com outros direitos, verificando-se uma violação simultânea a diversos valores constitucionais. Com isso, o início da tutela aos dados pessoais precede a Constituição Federal do Brasil, sendo paralela à proteção a demais liberdades individuais, como a intimidade, honra e sigilo de correspondências e comunicações. Contudo, a tutela constitucional autônoma de dados pessoais viabiliza uma proteção holística em detrimento de sua fragmentação em diversos elementos. Abrange o acesso e conhecimento de dados sobre si, direito de sigilo, identificação dos responsáveis pela coleta e sua finalidade, retificação de dados, regulamentação normativa e fática estatal e, por fim, a livre disposição de dados que dizem respeito a seu titular.[30]

Com isso, ressalta-se uma vertente positiva, mais atrelada ao livre desenvolvimento do indivíduo, com a noção de autodeterminação informativa. Quanto a esse prisma, Menke aponta o pioneirismo da Alemanha na temática, com a edição inicialmente em 1970 da primeira lei a dispor sobre o tema no estado de Hessen. Posteriormente, sobreveio legislação em âmbito nacional no ano de 1977. Do mesmo modo, o país germânico apresentou, desde então, maior desenvolvimento jurisprudencial e doutrinário no tocante ao caráter autônomo do direito fundamental à proteção de dados, como se verá no Capítulo seguinte.[31]

---

[30] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, pp. 485-497.

[31] MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira*, v. 5, n. 1, pp. 781-809, 2019, p. 782.

No Brasil, a tutela autônoma ao direito fundamental à proteção de dados apenas adquire contornos claros com o advento da LGPD, que traz em seu bojo a noção de autodeterminação informativa e reforça a autonomia do titular dos dados sobre seu uso, destinação e controle.

Mas foi apenas em 2020, quando do julgamento da Ação Direta de Inconstitucionalidade (ADI) n. 6387, que o Supremo Tribunal Federal reconheceu o direito fundamental à autodeterminação informativa, destacando-o dos demais valores constitucionais. Referida ADI foi proposta pelo Conselho Federal da OAB em face da Medida Provisória n 954/2020, na qual foi autorizado o compartilhamento de dados pessoais por empresas de comunicações diretamente ao Instituto Brasileiro de Geografia e Estatística. A Suprema Corte, na ocasião, declarou a inconstitucionalidade desse diploma normativo por não trazer mecanismos claros para controle da finalidade do compartilhamento de dados. Para tanto, referendou uma tutela constitucional autônoma aos dados pessoais no ordenamento, plasmando o direito fundamental à autodeterminação informativa, que se diferencia do prisma original da privacidade e intimidade para conferir verdadeiro controle do titular sobre a difusão de seus dados. Afinal, como todos os dados são relevantes na Era da Informação, seu titular não pode ficar alheio ao uso e destinação empregados a informações que lhe são concernentes.

Embora autores como Sarlet prefiram o termo genérico "proteção a dados pessoais" em detrimento da expressão "autodeterminação informativa", tem-se que na sociedade atual a relevância dos dados impulsionou sua tutela para uma posição de autonomia dentre o leque de direitos fundamentais,[32] que teve seu status devidamente reconhecido no ordenamento pátrio.

Finalmente, apenas em 2022 houve o reconhecimento explícito do direito fundamental à proteção de dados pessoais, inclusive no ambiente virtual, no bojo da Constituição Federal. Nesse contexto, deve-se ponderar que a construção jurídico-constitucional da proteção a dados pessoais (ou autodeterminação informativa) precede o grau de desenvolvimento atual do ambiente informático.[33] Isso porque o envio e armazenamento de informações pessoais pode ser efetuado por meios mecânicos, fotográficos ou pelo simples armazenamento não autorizado de documentos. De qualquer modo, surgem novos contornos com o impulsionamento virtual,

---

[32] Sarlet sinaliza que esse termo é mais abrangente, permitindo abarcar a proteção da privacidade e intimidade dos titulares, sem abrir mão de seu necessário vínculo com o direito ao livre desenvolvimento da personalidade. (SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, pp. 495-496).

[33] Sydow aponta que o meio virtual se torna uma espécie de 'meio ambiente artificial', criado a partir de intervenção e vontade humanas. Essa relação é evidenciada sob a ótica trabalhista, com forte progressão de atividades desempenhadas a distância, em sistema *home Office*, o que ocasiona verdadeiro ambiente de trabalho virtual. (SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, pp. 69-71).

em que a obtenção de dados ocorre em magnitude sem precedentes e instantaneamente. Com isso, o efetivo reconhecimento pátrio dessa tutela ocorreu dentro do contexto informático, em que se aprofundam os desafios com a criação de bancos de dados informatizados, perenes e de compartilhamento em tempo real, com maior potencial lesivo aos cidadãos.[34]

Por essa razão, na atualidade, uma adequada compreensão dessa tutela necessariamente perpassa por uma minuciosa análise do ambiente informático, que se torna o eixo de proteção e fomento às garantias atreladas aos dados pessoais.

Conforme aponta Sieber, os dados pessoais sofreram paulatina relevância à medida que a sociedade se desenvolveu. A origem desse processo remonta à Revolução Industrial, marcada pela substituição da força humana por máquinas e que estabeleceu nova relação entre capital e trabalho. Porém, a segunda grande revolução se inicia no século XX, com a transição da sociedade industrial para a sociedade da informação: agora, parte da atividade intelectual humana passa a ser substituída por máquinas dotadas de inteligência artificial.[35] Essa revolução teve sua raiz com a Internet, que estabeleceu um código de comunicação instantâneo que conecta todo o mundo por meio de uma linguagem comum (protocolos TCP/IP).[36] Na sociedade atual, com isso, o aspecto imaterial passa a adquirir maior valor, de modo que os dados se tornam os novos fatores de poder e riscos.[37]

Computadores estão incorporados no cotidiano e são uma das mais relevantes fontes de informação. Há uma integração global não apenas de mercados, mas também em rede, o que faz jus à expressão cunhada por Manuel Castells alusiva à sociedade em rede.[38] Governos passam a adotar sistemas informatizados para atividades cotidianas: uso da urna eletrônica para exercício do direito ao voto, sistemas são automatizados para maior celeridade em ações judiciais, houve aprimoramento do Datasus, com informações sobre a vacinação contra COVID-19.

Para os usuários, a informática viabiliza a aquisição de produtos, trabalho em home office e reuniões virtuais (muito popularizadas durante o período da pandemia de COVID-19), transações bancárias pelo *Internet Banking*, dispensando-se o deslocamento físico para

---

[34] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, p. 494.

[35] SIEBER, Ulrich. Computer Crime and Criminal Information Law: New Trends in the International Risk and Information Society. *COMCRIME Study*. European Commission, 1998. Disponível em: https://www.law.tuwien.ac.at/sieber.pdf. Acesso em 28 set. 2021.

[36] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 41.

[37] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 33.

[38] Cf. CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006, pp. 17-30.

inúmeras atividades diárias. A Internet se torna um novo ambiente[39] em que os indivíduos "constroem sua reputação virtual" (honra): realizam suas atividades cotidianas, interagem em redes sociais e armazenam diversos conteúdos de caráter pessoal (imagens, vídeos, documentos, pesquisas), tudo isso com expectativa de total autonomia de sua forma de utilização (privacidade e livre disposição).[40]

Convém, neste ponto, trazer breve e necessária observação: não há uma evolução informatizada uniforme e equânime na sociedade. Afinal, parcela significativa da população carece de provisões mais elementares para sua sobrevivência, como alimentação e moradia, sendo longínquo seu acesso à Internet. Nesse contexto, a análise desses contrastes deve ser inserida em qualquer análise acerca da sociedade da informação.[41] De qualquer modo, com o progresso da sociedade atual e sua conexão em rede, entende-se que o acesso à Internet deve ser erigido ao status de direito fundamental. Sem ele, hodiernamente não será possível o livre desenvolvimento da personalidade, em violação à dignidade da pessoa humana. Nesse sentido, Martins, que também adota esse posicionamento, aponta que a Finlândia foi o primeiro país a conferir ao direito à Internet o status de direito fundamental, em 2010.[42]

D'outra sorte, essa maior dependência dos cidadãos no tocante a sistemas informatizados também suscita maiores violações. Os riscos informáticos geram uma

---

[39] Não é compreendido como meio ambiente artificial em termos jurídicos (Lei 6938/81 obsta essa interpretação porque diz ordem física, química e biológica). Mas é um ambiente cultural efetivamente: ser humano nele constrói sua personalidade e se desenvolve.

[40] Tecnologias de blockchain para certificação de dados, transações. Conceito de vida virtual – avatar, personalidade própria e distinta na Internet. Turismo virtual. Cultura virtual: cinema, filmes, teatros.

[41] BRITO, Auriney. *Direito Penal Informático*. São Paulo: Saraiva, 2013, pp. 18-19. Não se olvida que as marcantes desigualdades sociais do país refletem também na seara digital, de maneira que ainda há significativo número de pessoas que nem sequer possuem acesso à Internet. No entanto, o montante de usuários com acesso à rede vem crescendo paulatinamente, sendo inexorável atingir a imensa maioria da população. Em abril de 2021, 82,7% da população brasileira possuía acesso à Internet no país, o que demonstra seu papel central no cotidiano. GOVERNO FEDERAL. Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à Internet. *Site do Governo Federal***.** 14 de abril de 2021. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=IBGE-,Pesquisa%20mostra%20que%2082%2C7%25%20dos%20domic%C3%ADlios,brasileiros%20t%C3%AAm%20acesso%20%C3%A0%20internet&text=A%20popula%C3%A7%C3%A3o%20brasileira%20est%C3%A1%20cada,Geografia%20e%20Estat%C3%ADstica%20(IBGE). Acesso em: 04 out. 2021. No mais, é notória a essencialidade do acesso à Internet – o que foi potencializado e catalisado pela pandemia de Covid-19 – para o cotidiano: atividades diárias como educação, trabalho, compras, acesso a contas bancárias, a o próprio acesso à informação. Disso se depreende que o simples acesso à rede passa a adquirir status de direito fundamental implícito, considerando ser pressuposto para adequada promoção da dignidade da pessoa humana (fundamento da República, nos termos do artigo 1º, inciso III, da Constituição Federal) e construção de uma sociedade livre, justa e solidária (objetivo fundamental da República, nos termos do artigo 3º, inciso I, da Constituição Federal). Logo, incumbe ao Estado a paulatina inclusão digital dos cidadãos.

[42] MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, p. 795. Ainda, foi aprovada pelo Conselho de Direitos Humanos da ONU a Resolução A/HRC/C/L.20 de 2016, que em seu artigo 2º: "reconhece a natureza global e aberta da Internet como uma força motriz na aceleração do progresso rumo ao desenvolvimento nas suas diversas formas, inclusive na realização de metas de desenvolvimento sustentável".

deterioração do pleno exercício dessas atividades, prejudicando a integridade dos arquivos armazenados no dispositivo e na nuvem, destruição da imagem virtual (e, dependendo da repercussão, imagem na realidade física), a violação à privacidade e à honra pessoal.[43] Estes são os valores particularmente expostos a risco no ambiente virtual, todos diretamente atrelados à autodeterminação informativa. Por essa razão, no bojo desse novo direito fundamental, há de se conferir destaque ao aspecto informatizado, o qual efetivamente pulveriza potenciais violações aos dados pessoais.

Alguns autores asseveram que, a partir das inúmeras lesões em potencial e de sua essencialidade, os direitos provenientes do ambiente virtual consistem em direito humano de quinta dimensão.[44] Tratar-se-ia de proteger o desenvolvimento da personalidade do indivíduo nesse novo ambiente. Ocorre que não há um consenso quanto a direitos de quarta ou quinta dimensão, sendo frequentemente reconduzidos às três primeiras dimensões.[45] Na hipótese em apreço, é notório que a proteção aos dados pessoais no ambiente virtual, como manifestação da autonomia dos indivíduos, remonta aos direitos de primeira dimensão.[46] É desnecessário, com isso, erigi-lo a patamar distinto dentro das dimensões de direitos humanos preceituadas por Karel Vasak.

Para a sociedade em rede e de risco atual, solução mais adequada para os novos desafios da tutela a dados pessoais no ambiente virtual consiste em reconhecer, no bojo do já consagrado direito à autodeterminação informativa – de primeira dimensão – as particularidades que cercam sua proteção informática: nela há maior potencial lesivo quando comparada à violação a informações fisicamente armazenadas, tanto em razão da interdependência da sociedade atual como também por força de sua instantaneidade e alcance global. Propõe-se, com isso, a autodeterminação informática como subcategoria desse direito fundamental, que adquire particular relevância no direito penal para a conformação de um novo bem jurídico. Elencam-se a seguir os principais fundamentos jurídicos para seu reconhecimento, que serão

---

[43] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 37.

[44] "Para José Alcebíades de Oliveira e Antonio Wolkmer tal dimensão trata dos direitos vinculados aos desafios da sociedade tecnológica e da informação, do ciberespaço, da Internet e da realidade virtual em geral." (*Curso de direito constitucional*. São Paulo: Saraiva, 2021, p. 822).

[45] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018, p. 337.

[46] Os direitos de primeira dimensão se referem a valores individuais e liberdades públicas, como a vida, propriedade. Nesses casos, o dever primevo do Estado consiste em não interferir na liberdade do indivíduo em respeito a seu livre desenvolvimento. Há, por outro lado, um dever secundário de agir, assegurando o pleno exercício pelos indivíduos em sociedade. Distingue-se, com isso, dos direitos de segunda e terceira dimensão, que são direitos socieais e transindividuais, respectivamente. (MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva, 2021, pp. 817-819).

desenvolvidos nos capítulos seguintes: a) a possibilidade de obtenção de dados pessoais a partir do próprio sistema informático, como dados de navegação ou localização do usuário, circunstâncias analisadas pelo Tribunal Constitucional Alemão em 2008, quando do julgamento do Caso da Busca Online (Capítulo 1.1.1.); b) a elaboração dos principais diplomas normativos pátrios voltada ao ambiente informático: o Marco Civil da Internet e a LGPD (Capítulos 1.2. e 1.3.); c) o enfoque da Convenção de Budapeste conferido à confidencialidade, integridade e disponibilidade de dados informáticos.

1.1.1. Decisões paradigmáticas do Tribunal Constitucional Alemão quanto à proteção de dados

A Alemanha apresentou profícuo desenvolvimento na proteção de dados, inicialmente não diretamente relacionada ao mundo virtual, porém acompanhando o desenvolvimento tecnológico e promovendo uma expansão paulatina desse direito da personalidade. Trouxe influências notórias ao reconhecimento do direito à autodeterminação informativa pelo Supremo Tribunal Federal em 2020, quando do julgamento da ADI n. 6387. Nesse contexto, merecem destaque dois julgados do Tribunal Constitucional Alemão: o Caso do Censo Demográfico (*Volkszählungurtei*l) de 1983[47] e o Caso da Busca Online (*Online Durchsuchung*) em 2008.[48] O primeiro caso consagrou o direito fundamental à autodeterminação informativa, enquanto o segundo reconheceu contornos próprios da tutela aos dados pessoais no ambiente informático.

O Caso do Censo Demográfico se originou do questionamento da constitucionalidade da Lei Federal de Recenseamento alemã de 1982, na qual, dentre outros aspectos, era facultado o armazenamento e compartilhamento de dados pessoais dos indivíduos pelo Estado Alemão a fim de se promover o recensemento da população. Nesse julgamento, o Tribunal Constitucional Alemão reconheceu a constitucionalidade da finalidade declarada da Lei. No entanto, reconheceu a inconstitucionalidade de diversos dispositivos que permitiriam armazenamento e transferência de dados pessoas dos indivíduos entre órgãos estatais.

O caráter paradigmático dessa decisão residiu em se reconhecer o direito fundamental à autodeterminação informativa (*Recht auf informationelle Selbstbestimmung*) com base nos

---

[47] DEUTSCHLAND. *Bundesverfassungsgericht. Verfassungsbeschwerde n. 209/83, 484/83, 440/83, 420/83, 362/83, 269/83*, 1. Senat, Karlsruhe, 15 dez. 1983. Disponível em: http://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 29 set. 2021.

[48] DEUTSCHLAND. *Bundesverfassungsgericht. Verfassungsbeschwerde n. 370/07*, 1. Senat, Karlsruhe, 27 feb. 2008. Disponível em: http://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em: 29 set. 2021.

artigos 2, I, e 1, I, da Lei Fundamental Alemã, consubstanciados pelo livre desenvolvimento da personalidade e pela inviolabilidade da dignidade humana.

Nesse julgado foi reconhecida a proteção do indivíduo contra o levantamento, armazenamento, uso e disposição de dados pessoais com base em um prisma dúplice. Por um lado, trata-se de centralizar no indivíduo o direito de decidir como e em quais limites informações a seu respeito serão divulgadas.[49] Em um segundo aspecto, o Tribunal reforça que a autodeterminação informacional pressupõe a liberdade de decisão e possibilidade de verificar quais informações estão sob alcance de terceiros e quem as detém. Isso implica empoderamento do titular, de modo a obstar controle de seu comportamento e ulteriores prejuízos a seu desenvolvimento autônomo.[50] [51]

Já no século XXI, com a disseminação de dispositivos informáticos na denominada Era da Informação, passou-se a notar que não apenas o Estado, como também particulares podem obter dados e utilizá-los em desfavor de seu titular. Isso porque, à medida que os computadores passam a desempenhar papel central no dia a dia dos indivíduos, surgem novos riscos aos direitos da personalidade.[52] Nesse novo contexto, quando do Julgado da Busca Online, em 2008, o Tribunal Constitucional Alemão deu um passo além para consolidar os direitos da personalidade dos indivíduos no ambiente virtual.

O pano de fundo para a análise do Tribunal consistiu no reconhecimento de que a regulamentação de acesso secreto a sistemas técnico-informáticos viola direito geral da personalidade, reconhecendo-se uma nova manifestação sob o prisma do direito fundamental à conservação da confidencialidade e integridade dos sistemas informáticos.[53] Assim, é vedada a busca ou investigação remota de computadores de pessoas suspeitas do cometimento de atos ilícitos sem autorização judicial legalmente embasada.

---

[49] DEUTSCHLAND. *Bundesverfassungsgericht. Verfassungsbeschwerde n. 209/83, 484/83, 440/83, 420/83, 362/83, 269/83*, 1. Senat, Karlsruhe, 15 dez. 1983. Disponível em: http://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 29 set. 2021, §144.

[50] DEUTSCHLAND. *Bundesverfassungsgericht. Verfassungsbeschwerde n. 209/83, 484/83, 440/83, 420/83, 362/83, 269/83*, 1. Senat, Karlsruhe, 15 dez. 1983. Disponível em: http://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 29 set. 2021, §146.

[51] Não se pode olvidar que o desenvolvimento informático naquela época se encontrava em momento embrionário, de modo que inexistia uma disseminação de dispositivos informáticos nas mãos de cada indivíduo. O enfoque voltou-se a uma inquietação da população no tocante a eventual controle por parte do Estado, tanto em razão do período de Guerra Fria, em que ainda vigorava embate com a Alemanha Oriental, como também pela proximidade temporal com o livro 1984, de George Orwell, que apontava para um Estado controlador. (HOFFMANN-RIEM, Wolfgang. Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzer informationstechnischer Systeme. *Juristen Zeitung*, vol. 21, n. 1, pp. 1009-1022, 2009, p. 1009).

[52] MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira*, v. 5, n. 1, pp. 781-809, 2019, p. 795.

[53] DEUTSCHLAND. *Bundesverfassungsgericht. Verfassungsbeschwerde n. 370/07*, 1. Senat, Karlsruhe, 27 feb. 2008. Disponível em: http://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em: 29 set. 2021, §166.

Na ocasião, a Corte sustentou inexistir direito fundamental já consagrado a assegurar referida garantia, diferenciando-a dos direitos à privacidade e da própria autodeterminação informacional, sendo necessário o preenchimento dessa lacuna em razão de novos avanços tecnológicos e mudanças no estilo de vida dos cidadãos.[54]

De início, o Tribunal reconheceu o papel central desempenhado pela informática no cotidiano, cujas novas possibilidades e riscos eram imprevisíveis no século anterior. Isso se deve à capacidade de armazenamento dos dipositivos, a seu emprego e implementação em todas as atividades diárias e à interconexão entre os dispositivos, maximizando a possibilidade de obtenção indevida de dados.[55] Com isso, o armazenamento desses dados é apto a trazer conhecimentos aprofundados sobre o usuário, inexistindo um método unívoco e absolutamente seguro de autoproteção.[56] Desse contexto dúplice de necessidades e riscos surge a imprescindibilidade de tutela de um novo direito fundamental.

O Tribunal ressaltou a incongruência dessa proteção com o direito da privacidade. Este se limita a vedar ingerências indevidas sobre aspectos internos do indivíduo. No entanto, a proteção a sistemas informáticos transborda a esfera privada, de modo que deve abarcar todos os dados aptos a fornecer fragmentos ou uma imagem geral do usuário.[57] Do mesmo modo, a autodeterminação informacional, direito da personalidade reconhecido no *Völkszählungsurteil*, apresenta um âmbito de aplicação distinto, posto que direcionado ao direito de o indivíduo decidir sobre a disponibilização e uso de dados pessoais, ampliando a liberdade de comportamento. Apesar de ser também direcionado a particulares e transbordar a mera proteção a dados sensíveis, não leva em consideração a vinculação entre o titular dos dados e os sistemas informáticos. É possível, assim, obtenção de informações sobre o próprio sistema de informação, como dados de navegação ou localização do usuário, não abarcados pela autodeterminação informacional.[58]

Por essa razão, com vistas a abranger o sistema informacional em sua totalidade,[59] reconheceu-se o direito fundamental à garantia da confiabilidade e integridade de sistemas, também derivada da dignidade da pessoa humana e do livre desenvolvimento da personalidade. Visa-se, assim, a vedar qualquer acesso ao sistema que possibilite acesso a um aspecto essencial

[54] Ibidem, §167, 169.
[55] DEUTSCHLAND. *Bundesverfassungsgericht. Verfassungsbeschwerde n. 370/07*, 1. Senat, Karlsruhe, 27 feb. 2008. Disponível em: http://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em: 29 set. 2021, §172-178.
[56] Ibidem, §180.
[57] Ibidem, §197
[58] Ibidem, §200.
[59] Ibidem, §203.

da forma de vida da pessoa ou de uma imagem de sua personalidade, vedando-se quaisquer propósitos não autorizados, de índole estatal, privada ou comercial.

Autores como Eifert sustentam ter sido prescindível a criação de um novo direito fundamental, sendo que a autodeterminação informativa poderia abarcar os novos preceitos atinentes ao sistema informático. Assim, não haveria uma lacuna de proteção, mas uma incidência concomitante do princípio da proporcionalidade para se perquirir sobre eventual lesão ao direito da personalidade por força do acesso a sistemas informáticos.[60]

De qualquer modo, muito embora se reconheça que se trata mormente de um desdobramento da autodeterminação informativa previamente reconhecida, é notório o avanço do tribunal na tutela da proteção de dados, ao abranger a confidencialidade, integridade e disponibilidade dos sistemas informacionais, porquanto indissociáveis dos direitos da personalidade na sociedade atual. Esse desenvolvimento propiciou o fomento do aspecto positivo da tutela de dados, tornando seu titular protagonista no exercício dos direitos dela decorrentes.

O Caso da Busca Online, assim, conferiu destaque a um prisma particular e essencial da autodeterminação informativa: sua proteção no âmbito informático, em que as violações possuem maior potencial de perfusão, considerando-se o grau de inserção da sociedade nesse novo ambiente. Logo, como defendido no Capítulo 1.1., essa proteção não se desvencilha do direito fundamental à autodeterminação informativa, porém realça a relevância de uma particular atenção ao ambiente informático.

A partir desse pioneiro e amplo desenvolvimento da jurisprudência alemã no decorrer de décadas, em um confronto com a tutela à proteção de dados no Brasil, há uma preocupação pátria tardia com o tema. Em sede da relação entre Direito e Informática, verifica-se que em nosso país ocorreu uma relação centrípeta e invertida: houve regulamentação a partir de seu segmento mais gravoso, penal, para posterior tutela cível e administrativa. De mais a mais, a aprovação da Lei n. 12.737/2012, criando tipificação para os delitos propriamente informáticos, foi oriunda de pressão populista após violação de dados de uma atriz nacional.

De qualquer modo, fato é que projetos legislativos acerca da elaboração de um crime informático eram discutidos há mais de dez anos no Congresso Nacional, sendo o evento supramencionado um catalisador para uma tutela necessária. Esse evento escancarou, ademais, a carência de regulação jurídica do ambiente virtual, o que impulsionou a aprovação do Marco Civil da Internet em 2014 e, mais recentemente, da LGPD. Por fim, apenas em 2020 foi

[60]EIFERT, Martin. Informationelle Selbstbestimmung im Internet: Das BVerfG und die Online-Durchsuchungen. *Neue Zeitschrift für Verwaltungsrecht*, v. 521, 2008.

reconhecido o direito fundamental à autodeterminação informativa, cuja tutela é norteada pelas preocupações alusivas ao ambiente informático. E sua consagração explícita no texto constitucional, como visto, ocorreu apenas em 2022, com a inclusão do artigo 5º, inciso LXXIX à Constituição Federal. Nos próximos Capítulos, visa-se a destacar aspectos relevantes dessas leis que possam impactar na proteção penal conferida aos dados pessoais no ambiente virtual.

1.2. Marco Civil da Internet

O tratamento do ordenamento jurídico pátrio à proteção extrapenal de dados foi tardio. Iniciou-se tão somente em 2014, com o advento da Lei n. 12.965/2014, impulsionada pela revelação de espionagem da Agência Nacional de Segurança norte-americana, por Edward Snowden. Com isso, por meio de princípios, o Marco Civil da Internet buscou trazer direitos mínimos aos usuários do meio virtual sem, contudo, impor legislação restritiva das liberdades individuais – inerente ao âmbito criminal –, o que culminaria com "efeitos inibitórios para a inovação e a dinamicidade da Internet."[61]

Verifica-se que a atenção legislativa à tutela de dados pessoais volta-se ao ambiente informático, do qual emergem os principais desafios para a proteção à autodeterminação informativa.

A partir de seu artigo 3º, estabeleceu-se um trinômio de valores ordenadores do sistema informático: neutralidade, privacidade e liberdade de expressão. Conforme apontam de Teffé e de Moraes, a neutralidade e a privacidade representam dois lados de uma mesma moeda: enquanto a primeira fomenta a liberdade de expressão, a privacidade estabelece algumas balizas para seu exercício.[62]

No mais, a liberdade de expressão, já assegurada no texto constitucional, recebe particular atenção pelo Marco Civil da Internet, o que se denota de seu resguardo como fundamento (artigo 2º) e princípio (artigo 3º), além de garantia prevista nos artigos 8º e 19º.

A partir dessa sistemática de tutela, verifica-se a delineação de todo o diploma normativo com vistas a assegurar o livre desenvolvimento da personalidade do usuário. Com

---

[61] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 183.

[62] DE TEFFÉ, Chiara Spadaccini; DE MORAES, Maria Celina Bodin. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Pensar-Revista de Ciências Jurídicas*, v. 22, n. 1, pp. 108-146, 2017, p. 112. A partir do princípio da neutralidade, impõe-se um tratamento uniforme e não discriminatório dos dados transportados e armazenados em rede, independentemente de seu conteúdo, origem, destino e do usuário (conforme disposto no artigo 9º). Do mesmo modo, veda-se o bloqueio, monitoramento, filtro ou análise de conteúdo de dados por meio da Internet (artigo 9º, §3º).

efeito, torna-se uma preocupação central permitir maior grau de controle do indivíduo sobre seus dados inseridos no ambiente informático, tendo em vista a mercantilização das informações no ambiente virtual.[63]

Com isso, o artigo 7º do Marco Civil da Internet elencou uma série de direitos do usuário para sua tomada de decisão livre e consciente, notadamente: a) a inviolabilidade da intimidade e vida privada, além do fluxo e conteúdo de comunicações; b) disponibilização de informações claras e completas sobre contratos de prestação de serviços de Internet; c) não fornecimento a terceiros de dados pessoais, com o devido e justificado esclarecimento acerca de seu armazenamento e emprego; d) consentimento livre, expresso e informado sobre coleta, uso, armazenamento e tratamento de dados pessoais.

Deve-se ponderar, a seu turno, algumas limitações no tocante à responsabilização de usuários e plataformas por ilícitos. Por um lado, o artigo 21 do Marco Civil da Internet foi demasiado restritivo ao estabelecer a responsabilidade subsidiária do provedor pela manutenção de conteúdos ilícitos, limitando-se a cenas de nudez e atos sexuais, o que ocorrerá tão somente após notificação judicial. Ademais, o período de armazenamento das informações por provedores de conexão e de aplicação e é demasiado curto (respectivamente, um ano, segundo o artigo 13, e seis meses, conforme o artigo 15), frequentemente obstando a devida identificação do infrator.

De qualquer modo, cotejando o teor global do Marco Civil da Internet, depreende-se a implementação do paradigma da autodeterminação informacional no tocante aos dados pessoais de usuários virtuais.[64] A promulgação tardia dessa lei resta evidente quando comparada ao reconhecimento de referido direito fundamental cerca de trinta anos antes pelo Tribunal Constitucional Alemão, em 1983.

1.3. Lei Geral de Proteção de Dados

Não obstante o mérito do Marco Civil da Internet ao apresentar pioneira tutela legislativa no ordenamento pátrio, a Lei n. 13.709/2018 propiciou importante avanço ao estabelecer um microssistema protetivo de dados pessoais, de modo a trazer extensa regulamentação e sanções de caráter civil e administrativo, sem excluir outros sistemas como o

---

[63] DE TEFFÉ, Chiara Spadaccini; DE MORAES, Maria Celina Bodin. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Pensar-Revista de Ciências Jurídicas*, v. 22, n. 1, pp. 108-146, 2017, p. 123.

[64] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 124.

Código de Defesa do Consumidor.[65] Sua tutela demonstra particular atenção aos dados no ambiente informático, que se torna o ambiente mais desafiador em razão de sua perfusão e interconexão instantânea.

Na linha dos direitos fundamentais que defluem da tutela de dados pessoais, conforme já reconhecido no Capítulo anterior, a LGPD reforçou sua vertente protetiva em face de ingerências alheias, estabelecendo como fundamentos a proteção à privacidade, intimidade, honra e imagem (artigo 2º, incisos I e IV).

A seu turno, conferiu-se particular destaque à manifestação ativa da autonomia do titular dos dados. O artigo 2º, inciso II, da LGPD consagrou expressamente o direito fundamental à autodeterminação informacional, cujo principal vetor é o consentimento do usuário (artigo 7º, inciso I, da LGPD).[66] Com isso, a LGPD conflui na linha do reconhecimento de um novo direito fundamental, conforme já plasmado no ordenamento alemão (alcunhado "autodeterminação informativa") e, em 2020, pelo Supremo Tribunal Federal.

O artigo 2º, inciso VII, por sua vez, plasma o livre desenvolvimento da personalidade como fundamento da tutela dos dados pessoais, o que destaca o reconhecimento do titular de dados como ser autônomo e protagonista, exercendo papel ativo quanto ao uso e destinação dos dados pessoais.[67]

A definição de consentimento encontra-se expressa na própria LGPD, qual seja: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (artigo 5º, inciso XII).

Dessa forma, o titular dos dados deve possuir conhecimento dos termos e condições de uso de qualquer funcionalidade no ambiente virtual, de forma clara e expressa, para então manifestar sua concordância.[68] O indivíduo se torna o "centro gravitacional"[69] da proteção conferida pela Lei, a ele competindo o controle e autorização do uso de seus dados pessoais.

---

[65] DE LIMA, Cintia Rosa Pereira; RAMIRO, Lívia Froner Moreno. Direitos do Titular dos Dados Pessoais. In: De Lima, Cíntia Rosa Pereira (coord). *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020, p. 249.

[66] A expressão "consentimento" é mencionada 37 vezes no decorrer dos 65 artigos da LGPD.

[67] Sobre tal fundamento, Saldanha discorre que: "a autodeterminação informativa abriga a filosofia de que o indivíduo titular de dados pessoais deve ser o protagonista das matérias relacionadas ao tratamento de seus dados pessoais, trazendo ao sujeito o foco das operações em preocupação perpétua com a privacidade." Desse modo, verifica-se que a intenção do legislador, ao fundamentar a LGPD na autodeterminação informativa, é conferir papel ativo aos cidadãos quanto ao uso de seus dados pessoais. (SALDANHA, João. *Fundamentos da LGPD: a autodeterminação informativa*. 2019. Disponível em: https://triplait.com/a-autodeterminacao-informativa/. Acesso em: 17 dez. 2021).

[68] DE LIMA, Cintia Rosa Pereira; RAMIRO, Lívia Froner Moreno. Direitos do Titular dos Dados Pessoais. In: De Lima, Cíntia Rosa Pereira (coord). *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020, p. 250.

[69] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 186.

Nesse esteio, o artigo 18 da LGPD acresce uma série de direitos ao titular dos dados pessoais, como: a) a confirmação da simples existência de tratamento de dados; b) acesso e correção de dados; c) anonimização, bloqueio ou eliminação de dados desnecessários ou em desacordo com a Lei; d) informação sobre a possibilidade de negativa de consentimento e as consequências dela decorrentes.[70]

De qualquer modo, Bioni tece críticas à sobrevalorização do consentimento, posto que há questionamento razoável à racionalidade dos usuários e a seu poder de negociação frente a empresas e ao Estado, o que obsta um efetivo controle de seus dados pessoais.[71] De fato, é de se reconhecer que os titulares, ao utilizar cotidiana e usualmente o ambiente informático, acabam por automatizar algumas de suas condutas, conferindo atenção reduzida ao tratamento conferido a seus dados pessoais em cada endereço eletrônico acessado. Ademais, frequentemente a principal consequência da negativa de consentimento consiste no total óbice de acesso à plataforma ou serviço almejado, o que não satisfaz às necessidades do usuário.

Por essa razão, Bioni sustenta a criação de mecanismos aptos a mitigar a responsabilidade que recai sobre o usuário, permeado por vulnerabilidades equiparáveis à do consumidor, quais sejam, técnica, informacional e econômica. Para tanto, mostra-se necessária uma regulamentação normativa do próprio fluxo informacional, além de implementar sistemas mais intuitivos e que auxiliem na tomada de decisão pelo usuário (denominado "soft paternalism").[72]

Essas observações, conquanto pertinentes na esfera cível e administrativa, recebem contornos distintos na esfera penal. Afinal, conforme aponta Bioni, a vulnerabilidade dos usuários deriva de uma economia que, por si só, se apropria dos dados pessoais em prol da lógica de mercado com vistas à obtenção de lucro.[73] Cite-se, a título exemplificativo, o compartilhamento de informações e dados de navegação entre três dos principais aplicativos e redes sociais utilizados: Whatsapp, Facebook e Instagram. Destarte, não há usuário protegido a partir de uma visão reducionista de seu consentimento. Por outro lado, na seara penal, a vulnerabilidade do usuário se fundamenta em um estado subjetivo ou condição pessoal do sujeito, como em crianças, idosos e pessoas com deficiência. Isso porque, nesse âmbito, o

---

[70] Ademais, não se está alheio à assimetria que costuma permear as relações na Internet, entre indivíduos, de um lado, e o Estado ou empresas, do outro. Por essa razão, surgem mecanismos corretivos, como: a) a necessidade de manifestação expressa; b) a vedação ao consentimento genérico (artigo 8º, §4º); c) o destaque de cláusulas referentes ao consentimento sobre o uso de dados (artigo 8º, §1º); revogabilidade a qualquer momento (artigo 8º, §5º); e) especial tutela a dados sensíveis (artigo 11) e referentes a crianças e adolescentes (artigo 14).

[71] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 188

[72] Ibidem, pp. 222-224.

[73] Ibidem, *loc. cit.*

tratamento de dados adquire características próprias à luz de cada caso concreto, o que o distingue do manejamento comercial conferido pelas empresas, lastreado em elevado volume de informações para amparar a tomada de decisões que maximizem seus lucros.

Por essa razão, nota-se a necessidade de abordagens distintas nessas esferas. Enquanto na tutela civil e administrativa é imprescindível maior regulamentação do próprio fluxo de informações, na esfera penal o enfoque recai sobre a identificação dos usuários vulneráveis, conferindo-lhes maior suporte para sua tomada de decisão. De qualquer modo, deve-se reconhecer a estreita relação entre os ramos jurídicos, de modo que incrementos na regulamentação global da Internet também implicarão redução da prática de delitos informáticos. Como se verá no Capítulo 4.2. (Criminologia e crimes informáticos), é imprescindível uma articulação entre todas as esferas para a efetiva prevenção delitiva. Do mesmo modo, a atuação do soft-paternalism também não pode ser descartada sob a ótica penal, de maneira que é necessário reconhecer hipóteses e sujeitos que devem receber especial tutela da norma penal – notadamente, vítimas jovens, idosas e ignorantes no que tange aos aspectos informáticos.[74]

1.4. Convenção de Budapeste

Como visto no Capítulo anterior, a tutela a dados pessoais adquire status incontestável e explícito de direito fundamental no ordenamento pátrio e em outros países, como a Alemanha, que trouxe os principais contornos a essa proteção, notadamente no ambiente informático. Como inspiração para delineamentos penais em diversos ordenamentos internos, na seara internacional, a Convenção de Budapeste[75] emerge como um reconhecimento da necessidade de particular tutela aos dados pessoais no ambiente informático, convergindo em direção a uma tutela penal uniforme. Trata-se de reconhecer que a proteção de dados pessoais adquire contornos próprios no ambiente informático, dado seu potencial lesivo e a interconexão global: nele se materializa a sociedade de risco atual. Aprofunda-se, ainda, em delitos tradicionais que passam a ser praticados pela via virtual e adquirem maior perfusão – os denominados delitos informáticos impróprios.

---

[74] Cf. Capítulo 4.4 (Proposta de classificação da vítima informática).

[75] CONSELHO DA EUROPA. *Convenção sobre o Cibercrime*, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 set. 2021.

A Convenção de Budapeste foi o primeiro tratado internacional sobre crimes informáticos (denominados *computer crimes*). Do mesmo modo, ajudou a plasmar um novo bem jurídico-penal tutelado, que se desdobra nas vertentes de confidencialidade, integridade e disponibilidade de sistemas e dados informáticos,[76] conforme reconhecido em seu preâmbulo e no título 1 dos crimes em espécie.[77] Assim, a Convenção de Budapeste segue a linha predeterminada do direito fundamental à tutela de dados – sob a ótica informática, em razão da instantaneidade e omnipresença desse novo ambiente – como lastreada na autodeterminação informativa, fruto do livre desenvolvimento da personalidade. A seguir, inicia-se a abordagem penal dessa tutela, partindo-se dos principais delitos previstos na Convenção, o que viabilizará extrair o bem jurídico-penal particularmente protegido no ambiente informático (Capítulo 2).

A primeira seção do Capítulo II da Convenção traz uma abordagem do direito penal material, de modo a postular uma uniformização de tratamento no âmbito internacional quanto aos crimes informáticos. Todos os delitos são propostos na modalidade dolosa, de modo a selecionar apenas as condutas mais gravosas na seara internacional. Não se pode olvidar esforços para punição de concurso de agentes em todos os crimes (artigo 11.1), bem como da modalidade tentada em parte significativa das tipificações sugeridas (artigo 11.2).

A primeira proposta de criminalização, constante do artigo 2º da Convenção, guarda relação com o acesso ilegítimo ao sistema informático, tipificado pelo artigo 154-A, do Código Penal. As exigências do crime de invasão de dispositivo informático no tocante à necessária violação de dispositivo de segurança, bem como aos elementos subjetivos especiais – apesar das críticas lançadas no Capítulo 3.4.1.2 (Figura equiparada a invasão de dispositivo informático) –, encontram amparo na Convenção, a qual faculta aos Estados membros a inclusão desses elementos. Na seara eleitoral, Brito, aponta também a correlação com o artigo 72, inciso I, da Lei n. 9.504/1997.[78]

Na sequência, o artigo 3º da Convenção de Budapeste propõe a criminalização da interceptação ilegítima de dados informáticos, conduta criminalizada no ordenamento pátrio pelo artigo 10, da Lei n. 9.296/1996, consistente na interceptação de comunicações de informática ou telemática.

A seu turno, o artigo 4º estipula a tipificação de condutas destinadas a danificar, apagar, deteriorar, alterar ou eliminar dados informáticos, denominada "interferência em dados". Essa

[76] Vide Capítulo 2.2.
[77] Muito embora o Brasil ainda esteja em processo de ratificação do acordo, sua influência sobre os tipos penais no ordenamento pátrio foi notória, com a compatibilização de vários dispositivos, notadamente no tocante à tipificação de condutas.
[78] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 59.

conduta, sintetizada como dano informático, não encontra correlação no ordenamento pátrio, dado não se enquadrar no clássico delito de dano previsto no artigo 163, do Código Penal, como se verá no Capítulo 3.4.3 (Crimes informáticos patrimoniais impróprios e mediatos).

A interferência em sistemas informáticos é coibida no artigo 5º, da Convenção de Budapeste, voltada à violação a um sistema concreto, mediante ataques de *Denial of Service* ou inclusive mediante inserção ou destruição de dados. No Brasil, não se verifica tipificação suficientemente abrangente, considerando-se que o artigo 266, §1º consiste em crime contra a incolumidade pública e, portanto, pressupõe uma aptidão a prejudicar número indeterminado de pessoas – requisito não constante da Convenção.

O artigo 6º denomina de uso abusivo de dispositivos condutas de produção, posse ou disponibilização de programas ou *hardwares* voltados à prática dos delitos previstos nos artigos 2º a 5º (acesso ilegal, interceptação ilegal, interferência em dados e interferência de sistemas), bem como senhas e códigos de acesso com essa finalidade. Essa conduta é parcialmente tipificada no ordenamento no artigo 154-A, §1º, do Código Penal.

No título 2, a Convenção de Budapeste prevê "infrações relacionadas com computadores", tratando-se de crimes informáticos indiretos ou mediatos. Assim, o artigo 7º estabelece a penalização da falsidade informática, consistente na alteração ilegítima de dados com intenção de uso para fins legais, como se fossem autênticos. Como aponta Brito, a conduta será típica no ordenamento pátrio caso haja alteração de documento público ou particular, enquadrável nas condutas de falsidade ideológica ou falsificação material de documento.[79] Se praticada por funcionário público, há possibilidade de configuração do crime de inserção de dados falsos em sistema de informações (artigo 313-A, do Código Penal). Não se tratando de alteração de documento, a conduta será atípica.

O artigo 8º, constante desse mesmo título, propõe a criminalização de condutas que culminem com a perda de bens de terceiros, mediante alteração de dados informáticos ou intervenção em sistema informático. Em sentido técnico, referida conduta se amolda no artigo 155, §4º-B, ou seja, furto qualificado mediante fraude por meio de dispositivo informático ou eletrônico. Neste ponto, portanto, desnecessária qualquer alteração legislativa.

Os títulos 3 e 4 da Convenção propõem a tipificação de delitos informáticos impróprios *stricto sensu*,[80] os quais foram fortemente impulsionados pelos meios digitais. Nesse esteio, o artigo 9º sugere a tipificação de infrações relacionadas com pornografia infantil. Essas condutas

[79] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 62.
[80] Cf. Capítulo 3.3. (Nomenclatura e classificação dos crimes informáticos).

encontram ampla previsão no Estatuto da Criança e do Adolescente.[81] Em reforço a outros diplomas internacionais, o artigo 10º dispõe a criminalização de violação de direitos autorais e direitos conexos praticados em ambiente virtual. No ordenamento pátrio, o artigo 184, do Código Penal tipifica violação de direito autoral.

[81] Artigos 241, 241-A, 241-B e 241-C.

2. NOVO BEM JURÍDICO TUTELADO NO AMBIENTE VIRTUAL

No Capítulo anterior foram estabelecidas as premissas constitucionais do direito fundamental da proteção de dados pessoais. Como se pode constatar, sua tutela emergiu inicialmente sob um prisma negativo-protetivo, evitando-se ingerência alheia sobre os direitos e garantias individuais. No entanto, paulatinamente houve um movimento rumo a sua tutela positiva com destaque para o ambiente virtual, fincada no direito fundamental ao livre desenvolvimento do indivíduo, manifestação essencial do direito à liberdade como defluência da dignidade da pessoa humana. Como principal manifestação da sociedade de risco na tutela de dados pessoais, a proteção à autodeterminação informativa no ambiente informático se torna o centro gravitacional de tutela dos ordenamentos nacionais e sob a ótiva internacional – como se extrai da Convenção de Budapeste.

Fincadas as balizas constitucionais e legais da proteção de dados pessoais no ambiente informático, no presente Capítulo impende extrair o bem jurídico-penal a ele atrelado, cujo caminho foi traçado pela Convenção de Budapeste, que realça o aspecto positivo dessa tutela sob o prisma da disponibilidade dos dados. Para tanto, será traçado breve histórico acerca da teoria do bem jurídico e a importância de sua manutenção na atualidade sob a vertente constitucional, para então se traçar a autodeterminação informática como o bem jurídico digno de tutela penal.

2.1. Breve escorço sobre a teoria do bem jurídico

A teoria do bem jurídico diz respeito ao conceito material do delito, de modo a fornecer uma justificativa da tipificação penal para a sociedade. O bem jurídico, com vistas à limitação do *ius puniendi*, torna-se a pedra angular legitimadora do sistema penal no Estado Democrático de Direito.[82] Precursores da noção de bem jurídico apenas aparecem com o Iluminismo, sobretudo por meio da obra de Cesare Bonesana, Marquês de Beccaria, ao buscar dissociar o direito penal de noções autoritárias, como lesa à majestade e violação aos mandamentos de divinos.[83]

Birnbaum cunhou pela primeira vez o termo "bem jurídico" no século XIX, com o intuito de abarcar um conjunto de valores do Estado Liberal, cuja ofensa ensejaria punibilidade.

---

[82] BECHARA, Ana Elisa Liberatore Silva. O rendimento da teoria do bem jurídico no direito penal atual. *Revista Liberdades*, v. 1, n.1, pp. 16-29, 2009, p. 16.
[83] Cf. *Dos delitos e das penas*. Trad. Luciana Guidicini e Alessandro Contessa. São Paulo: Martins Fontes, 2005.

Trata-se de uma densidade individualista, associando-se a noção de bem jurídico a interesses individuais fundamentais. A noção de delito emana como uma lesão aos direitos subjetivos dos cidadãos dessa sociedade, ideia a partir da qual Feuerbach supera o postulado de crime como pecado contra Deus ou ofensa ao monarca. Em acréscimo a Feuerbach, Birnbaum alega que não há uma lesão simplesmente a direitos subjetivos, mas sim a bens.[84]

Com a delineação por Birnbaum, Binding se desvincula do Iluminismo, filiando-se à escola positivista, de modo a postular que o bem jurídico consiste em tudo o que se encontra definido em lei, não em interesses sociais.[85] Von Liszt, inaugurando uma linha naturalística sociológica do positivismo, opõe-se à ideia de bens jurídicos derivados de decisões legislativas, bem como rejeita a ofensa aos bens jurídicos como uma lesão ao Estado. Segundo esse autor, o escopo do Direito Penal é a proteção de interesses sociais fundamentais, não provenientes do ordenamento jurídico em que cada um se insere, mas previamente estabelecidos.[86]

A noção de bem jurídico passou por teorias negativistas, com destaque para a Escola de Kiel, ao afastar teorias liberais e conferir lastro para a ascensão do fascismo. Na segunda metade do século XX, a escola de Baden se desvincula do pensamento positivista, segundo o qual conteúdo do delito é definido partir da lei. Desenvolveu-se uma concepção de direito prévio ao ordenamento jurídico, não como interesses sociais, mas inserida no mundo subjetivo de valores culturais. No entanto, trata-se de fórmula vazia de conteúdo, não sendo adequada à delimitação do *ius puniendi* estatal.[87]

Após a segunda Guerra Mundial, Welzel capitaneou a retomada de concepções jusnaturalistas, com o desenvolvimento do ontologismo em busca de compreensão da natureza das coisas prévia ao direito. Contudo, Welzel confere excessivo enfoque sobre a teoria da ação, deixando de destacar o bem jurídico como centro da teoria do delito.[88]

Finalmente, a evolução da noção de bem jurídico culminou com as teorias modernas, em duas vertentes principais: sociológicas e constitucionais. Hassemer, Amelung, Jakobs e Habermas são representantes da primeira escola, enquanto Roxin e Rudolphi são os principais expoentes da vertente constitucional.

---

[84] BECHARA, Ana Elisa Liberatore Silva. O rendimento da teoria do bem jurídico no direito penal atual. *Revista Liberdades*, v. 1, n.1, pp. 16-29, 2009, pp. 17-18.
[85] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, p. 183.
[86] BECHARA, Ana Elisa Liberatore Silva. *Op. cit.*, p. 18.
[87] Ibidem, p. 19.
[88] SOUZA, Luciano Anderson de. *Op. cit.*, pp. 183-184.

Amelung propõe a fundamentação do Direito Penal na teoria sociológica da convivência humana, ao passo que as condutas proibidas derivam de uma valoração de danosidade social.[89] Jakobs, em oposição a Amelung, postula a equivalência entre a norma e o conceito de bem jurídico, a fim de possibilitar uma integração sociológica e normativa. Contudo, essa identidade de conceitos estabelece um Direito Penal fechado em si mesmo, em contraposição à sua necessária abertura a sistemas pré-jurídicos.[90]

Hassemer e Habermas, a seus turnos, recorrem a noções atreladas à violação de interesses sociais: para o primeiro autor, são necessários danos sociais para ação do Estado, sempre a partir de orientação político-criminal; para Habermas, adepto da teoria do consenso social, deve haver um consenso entre os cidadãos acerca da reprovabilidade daquela conduta.[91]

A vertente constitucionalista, por outro lado, sustenta que a tarefa primária de delimitação de bens jurídicos é atribuída à Constituição, que fundamenta a liberdade individual, confere limitações ao poder estatal, bem como estabelece valores político-criminais a serem concretizados.

Como aponta Bechara, a vertente constitucionalista é aquela que melhor se amolda ao Estado Democrático de Direito. Viabiliza-se um escopo não apenas de interpretação das normas penais, mas de limitação à criminalização primária estatal. O conteúdo do bem jurídico compatível com essa estrutura deve ser proveniente de prescrições jurídicas prévias à legislação penal, de modo a vincular o legislador a determinados critérios. Não se trata de buscar uma origem no jusnaturalismo ou nas relações sociais prévias ao ordenamento jurídico, mas de se fundamentar na própria Constituição.[92] Por conseguinte, o bem jurídico é válido e necessário quando provém de um valor constitucional e prévio à normatização penal. Nessa linha de raciocínio, os bens jurídicos no âmbito do Direito Penal consistem em concretizações do conteúdo constitucional dos direitos fundamentais.[93]

---

[89] COSTA ANDRADE, Manuel da. *Consentimento e Acordo em Direito Penal*. Coimbra: Coimbra, 2004, p. 97. A doutrina teórica de Amelung, contudo, apresenta equívocos teóricos e pode acarretar consequências perniciosas à política criminal. Embora Amelung visasse a dispensar a relevância do bem jurídico, apenas reforçou a importânciado conceito para retirar a contingência valorativa do legislador. Amelung, nesse sentido, retoma ao positivismo de Binding que buscava superar. Em verdade, a importância do bem jurídico supera a relevância da teoria de danosidade social. A maior relevância de Amelung consiste, então, em postular uma abertura do Direito Penal às finalidades sociais. (COSTA ANDRADE, Manuel da. *Consentimento e Acordo em Direito Penal*. Coimbra: Coimbra, 2004, pp. 103-104).

[90] Ibidem, p. 117-118.

[91] SILVEIRA, Renato de Mello Jorge. *Direito Penal Supraindividual. Interesses difusos***.** São Paulo: Revista dos Tribunais, 2003, pp. 48-49.

[92] BECHARA, Ana Elisa Liberatore Silva. O rendimento da teoria do bem jurídico no direito penal atual. *Revista Liberdades*, v. 1, n.1, pp. 16-29, 2009, p. 19.

[93] Ibidem, p. 20.

Deve-se ponderar, no entanto, que os bens jurídicos não são social ou historicamente fechados.[94] Em verdade, são mutáveis ao passo que em cada momento social se determinam interesses fundamentais para o desenvolvimento livre na sociedade, tornando-se verdadeiro um padrão crítico de delimitação da legitimidade do Direito Penal em cada caso.[95] Nota-se que os próprios preceitos constitucionais não devem ser interpretados de forma restrita, de modo a permitir uma compatibilidade com a perspectiva social de cada momento histórico.[96]

Destarte, conforme Roxin, os bens jurídicos são "circunstâncias dadas ou finalidades úteis ao indivíduo e seu livre desenvolvimento no marco de um sistema social global estruturado sobre a base dessa concepção dos fins e para o funcionamento do próprio sistema."[97]

Extrai-se do raciocínio de Roxin a noção de que os bens jurídicos servem ao desenvolvimento de seu titular, de modo que, se uma conduta está baseada em uma disposição de seu portador, trata-se de pura expressão de sua personalidade, não havendo que se falar de prejuízo a seu livre desenvolvimento.[98]

Contudo, conquanto a concepção pessoal do bem jurídico possibilitou uma delimitação da intervenção penal, essa ótica conceitual não é mais capaz de abranger todas as decisões legislativas da sociedade atual.[99–100]. Nessa linha, Roxin aponta também o surgimento do Direito Penal do risco, a conduzir a incriminações mais amplas no campo prévio e com bens cada vez mais inapreensíveis. Indaga-se, com isso, até que ponto o direito penal do risco está em condição de fazer frente com seu tradicional instrumento liberal e ajustado ao Estado de Direito aos riscos modernos da vida.

Não se pode renunciar totalmente ao Direito Penal no campo do risco, porém deve ser preservada a referência ao bem jurídico e aos demais princípios constitucionais.[101] Por essa razão, conforme sustenta Bechara, deve-se estabelecer parâmetros seguros para uma efetiva limitação penal na atualidade, a fim de resguardar a não intervenção penal onde não se fizer

---

[94] A concepção é normativa, porém não é estática, pois dentro do marco das finalidades constitucionais está aberta às mudanças sociais e aos progressos do conhecimento científico.
[95] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, p. 57.
[96] BECHARA, Ana Elisa Liberatore Silva. O rendimento da teoria do bem jurídico no direito penal atual. *Revista Liberdades*, v. 1, n.1, pp. 16-29, 2009, pp. 20-21.
[97] Tradução livre do original: "circunstancias dadas o finalidades que son útiles para el individuo y su libre desarollo em el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del próprio sistema." (ROXIN, Claus. *Op. cit.*, p. 56).
[98] ROXIN, Claus. *La teoría del delicto en la discusión actual*. Tradução de Manuel Abanto Vásquez. Lima: Grijley, 2007, p. 268.
[99] BECHARA, Ana Elisa Liberatore Silva. *Op. cit.*, p. 26.
[100] O próprio Roxin, veemente defensor da teoria do bem jurídico, reconhece a incidência do direito penal em determinadas esferas em que inexiste um bem jurídico tutelado, como proteção de plantas e animais, embriões, proteção de futuras gerações. (COSTA, Helena Regina Lobo da. *Proteção penal ambiental: viabilidade, efetividade, tutela por outros ramos do direito.* São Paulo: Saraiva, 2010, p. 13).
[101] ROXIN, Claus. *Op. cit.*, pp. 60-61.

exigível uma proteção, em observância ao princípio da intervenção mínima.[102] Em particular, essa expansão deve ser refreada em bens jurídicos individuais que, conquanto inseridos no âmbito da sociedade de risco, devem se lastrear no livre desenvolvimento da personalidade do indivíduo: deve-se permitir, com isso, a assunção de riscos por seu titular sem que se dê ensejo à incidência necessária da tutela penal.

Todas propostas de abandono da teoria do bem jurídico foram vagas e desprovidas de conteúdo concreto, sendo inaptas a impor mecanismos seguros de contenção do *ius puniendi*. Assim, o bem jurídico consiste atualmente no melhor mecanismo material, lastreado em critérios constitucionais, para justificar e conferir constante autocrítica ao direito penal. [103]

2.2. Bem jurídico autodeterminação informática

Os valores socialmente tutelados se alteram de acordo com a época e a sociedade em que inseridos.[104] Assim, o direito penal não pode permanecer alheio a essa dinamicidade, devendo descriminalizar condutas em que houve perda de relevância, bem como – por outro lado – estar atento ao erigimento de novos bens jurídicos.

Conforme aponta Bechara,[105] os bens jurídicos não são forçosamente fixados anteriormente perante o legislador – podem, aliás, ser criados por ele. Trata-se de uma dinamicidade constante para a consecução de finalidades constitucionais conforme a realidade social verificada. Sem embargo, impõe-se redobrada cautela ao se propor o surgimento de novo bem jurídico, porquanto referida realidade implica a elaboração de novos tipos penais. Posto isso, o novo bem jurídico *sub judice* deve se compatibilizar com os princípios da intervenção mínima, fragmentariedade e *ultima ratio*, que guiam um Direito Penal mínimo, único caminho condizente com os vetores constitucionais e com as garantias individuais.

De qualquer modo, Silva Sánchez e Morán[106] apontam que surgem, de fato, novos bens jurídicos dignos de tutela penal, sem que isso implique violação aos princípios clássicos penais. Isso ocorre à contrariedade de outras causas de expansão do direito penal, como a pulverização

---

[102] BECHARA, Ana Elisa Liberatore Silva. O rendimento da teoria do bem jurídico no direito penal atual. *Revista Liberdades*, v. 1, n.1, pp. 16-29, 2009, pp. 26-27.
[103] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, pp. 187-188.
[104] BRITO, Auriney Uchôa de. O bem jurídico-penal dos delitos informáticos. *Boletim IBCCRIM*, São Paulo, v. 17, n. 199, pp. 14-15, jun. 2009, p. 14. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=71060. Acesso em: 15 ago. 2020.
[105] BECHARA, Ana Elisa Liberatore Silva. *Bem jurídico-penal*. São Paulo: Quartier Latin, 2014, pp. 122-123.
[106] SILVA SÁNCHEZ, Jesús-María; MORÁN, Ángel José Sanz. *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*. Madrid: Civitas, 2001.

de delitos de perigo, bens jurídicos supraindividuais, administrativização do Direito Penal, movimentos punitivistas derivados de ONGs e grupos coletivos.

Dessa forma, os avanços tecnológicos catalisados pela Revolução Industrial e fortemente impulsionados no século XX culminaram com o surgimento de diversos novos riscos em dimensões sem precedentes. Como aponta Beck, modernizam-se as premissas da sociedade anterior, de toda a ciência e da tecnologia, o que acarreta alterações sobre o cotidiano.[107] Para o autor, os riscos produzidos não se limitam a um âmbito fabril ou regional, mas apresentam uma característica inerentemente globalizada, de forma a superar fronteiras nacionais e acarretam ameaças supranacionais. Enquanto a sociedade industrial regia-se sobre o parâmetro de dominação da produção de riscos pela produção de riqueza, essa relação se inverte na sociedade atual.[108]

Na acepção de Merino Herrera, a noção de risco deve ser compreendida como um fenômeno social, em que há ponderações em uma relação custo-benefício: trata-se de consequências negativas evitáveis de certas decisões humanas.[109] Deve-se pontuar que riscos sempre permearam a história da humanidade, remontando-se a fases pré-industriais, como nas Grandes Navegações, bem como com o advento da Revolução Industrial.

No entanto, outrora imprevisíveis, atualmente busca-se controle e quantificação dos riscos, que também adquirem escalas sem precedentes e ignoram distâncias físicas, predominando a equidistância.[110] Pode-se elencar riscos atômicos, energéticos, ecológicos, financeiros e, em franca expansão, os riscos informáticos.

Nesse contexto, o ambiente virtual concentra significativa parcela dos riscos anunciados por Ulrich Beck, tendo em vista a progressiva informatização de todas as atividades cotidianas de indivíduos, empresas e Estados. A *Internet of Things* (IOT) conduz à interconexão entre inúmeros dispositivos (como veículos, aviões, drones, televisões) por meio da rede. Assim, paralelamente ao progresso inaurugurado, a Internet também é um fato criminógeno, impulsionando a proliferação de inúmeras atividades criminais.[111]

---

[107] BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. Tradução: Sebastião Nascimento. São Paulo: Editora 34, 2011, p. 13.
[108] Ibidem, p. 16.
[109] MERINO HERRERA, Joaquín. *Tendencias de la política criminal contemporânea*. Madrid: Marcial Pons, 2018, pp. 181-182.
[110] Ibidem, pp. 183-184.
[111] Ibidem, pp. 197.

De início, é fato, a informática consistiu essencialmente em mero instrumento para a prática de crimes tradicionais, como ameaça, crimes contra a honra e estelionato.[112]

Ocorre que, paulatinamente, os indivíduos, bem como a sociedade em geral, têm se tornado cada vez mais dependentes da informática. Atualmente, é notória sua inserção no cotidiano individual, com a intensificação de relacionamentos a distância, estudos, atividades profissionais e transações econômicas. Em um aspecto nacional e global, emerge seu protagonismo em todas as áreas econômicas, políticas, sociais e culturais. Nos termos propostos por Sieber, emergiu a Sociedade da Informação, conferindo-se importância a bens imateriais e grande dependência à rede informática.[113] Como as informações e a comunicação transpassam fronteiras, desvelando uma interconexão, Castells traz a noção de sociedade em rede:

> A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes.[114]

Essa crescente relevância na sociedade culminou com a prática de condutas lesivas aos direitos individuais, porém sem a correspondente tutela penal a partir dos delitos preexistentes. Cite-se, a título exemplificativo, a invasão de dispositivo informático com o apoderamento de dados pessoais, sem qualquer destruição do suporte físico em que armazenados, conduta que não pode ser tipificada como furto, à luz do princípio da legalidade.[115]

Assim, novas formas de violação à comunicação, troca e armazenamento de informações não se enquadram nos bens jurídicos preexistentes, como aquele tutelado pelo delito de violação de correspondência (artigo 151 do Código Penal). Nessa linha, mostra-se relevante a tutela de ações novas violadoras de dados, estes compreendidos como informação armazenada nos dispositivos informáticos,[116] bem como do suporte físico no qual a informação é veiculada.[117]

---

[112] BRITO, Auriney Uchôa de. O bem jurídico-penal dos delitos informáticos. *Boletim IBCCRIM*, São Paulo, v. 17, n. 199, pp. 14-15, jun. 2009, p. 14. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=71060. Acesso em: 15 ago. 2020, p. 15.

[113] SIEBER, Ulrich. Computer Crime and Criminal Information Law: New Trends in the International Risk and Information Society. *COMCRIME Study*. European Commission, 1998. Disponível em: https://www.law.tuwien.ac.at/sieber.pdf. Acesso em 28 set. 2021.

[114] CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006, p. 20.

[115] Cf. Capítulo 3.4.3. (Crimes informáticos patrimoniais impróprios e mediatos).

[116] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 22.

[117] NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 3, 4. ed. Rio de Janeiro, Forense, 2019, p. 335.

Com efeito, na linha da vertente constitucionalista da teoria do bem jurídico, a tutela aos dados pessoais encontra lastro no artigo 5º, inciso LXXIX, da Constituição Federal, consagrando-se sua autonomia como direito fundamental, com particular destaque ao ambiente digital, conforme mencionado na parte final desse dispositivo legal. Seu reconhecimento derivou, inicialmente, do artigo 5º, inciso X, da Carta Maior, porquanto consiste em um dos prismas da garantia à intimidade, privacidade, honra e imagem dos indivíduos, conforme escrutínio elaborado no Capítulo 1.1. (Desenvolvimento de um novo direito fundamental e sua construção constitucional). Ainda, o artigo 5º, inciso XII, assegura expressamente a inviolabilidade do sigilo dos dados. Por fim, não se pode olvidar a proteção genérica à liberdade conferida pelo artigo 5º, inciso II, que também se estende ao ambiente virtual. Como visto, esse direito fundamental adquiriu uma vertente ativa e de protagonismo de seu titular, compreendida como a autodeterminação informativa.

Essa tutela adquire contornos próprios em sede informática, símbolo da sociedade em rede e de risco. Destarte, justifica-se a tutela de um novo bem jurídico para assegurar-se o livre desenvolvimento da personalidade dos indivíduos em sociedade, uma vez que o manejo dos dados pessoais no ambiente informático se tornou imprescindível na sociedade atual e adquiriu status de direito fundamental explícito – e com destaque particular quando comparado ao tratamento de dados pessoais em geral, conforme expressa disposição constitucional, donde decorre o reconhecimento de sua autonomia e extravasamento com relação a outros valores constitucionais. E esse manejo se desgarra da tutela à autodeterminação informativa em geral, que abrange a tutela a dados não inseridos no ambiente informático. Isso porque, nestes casos, o potencial de impacto à esfera individual é menor, bem como progressivamente se reduz, considerando-se a paulatina informatização em todos os âmbitos da sociedade. Destarte, tendo em vista os particulares impactos da rede interconectada em tempo real sobre os dados pessoais, é de particular relevância sua tutela específica, também sob a ótica penal. Trata-se, com isso, de efetiva consagração ao princípio da fragmentariedade,[118] posto que se seleciona, dentro do direito fundamental à autodeterminação informativa, apenas as violações mais graves aos dados pessoais como dignos de tutela penal autônoma. Isso se traduz em um reconhecimento específico da proteção de dados no ambiente informático, abstendo-se de uma incidência penal autônoma diante de violações a dados pessoais fora desse ambiente.

Referida realidade é corroborada pela especial tutela aos dados pessoais em âmbito informático conferida em âmbito internacional pela Convenção de Budapeste, reconhecendo-

[118] Cf. Capítulo 2.4.

se que no ambiente virtual se materializam os principais interesses dignos de tutela penal e fomentadores às liberdades do indivíduo no manejo de seus dados. Com isso, a Convenção trouxe contornos mais nítidos à tutela penal das informações e dados no ambiente informático. Dispõe, em seu primeiro título, sobre a necessidade de criminalização de condutas que atentem à integridade, disponibilidade e confidencialidade das informações e dos sistemas no ciberespaço, o que sem sido amplamente adotado legislativa e doutrinariamente, a viabilizar uma uniformização internacional.

Por integridade dos dados e sistemas entende-se sua conservação, manutenção intacta das informações conforme definidas pelo usuário autorizado. A confidencialidade diz respeito à natureza privada das informações digitais, que apenas perdem esse caráter mediante autorização de acesso franqueada por seu titular. [119] Por fim, como disponibilidade entende-se a faculdade de acessar, utilizar, alterar, enviar, ou mesmo destruir dados livremente quando desejado por seu titular, consagrando diferentes formas de manifestação do livre desenvolvimento de sua personalidade. Este terceiro elemento visa a abarcar ainda eventuais sobrecargas de sistemas que obstem o uso adequado do dado (como *Denial of Service* que obste acesso à nuvem) ou mesmo a encriptação de dados (que com frequência cuminam com a prática do delito de extorsão).[120]

A partir desse prisma tripartite delineado pela Convenção de Budapeste, também inspirado em Sieber,[121] autores como Rossini,[122] Sydow [123] e Brito[124] defendem que o bem jurídico tutelado seria a segurança informática. Ocorre que o termo "segurança" não é apto a sintetizar com precisão a gama de lesões a que suscetíveis os dados e seus suportes informáticos. Afinal, mediante um ataque cibernético com posterior criptografia, a informação pode permanecer segura, ou seja, íntegra e confidencial, mas inacessível. Dessa forme, entende-se que o termo "segurança informática" não abarca com precisão a vertente de disponibilidade desse novo bem jurídico.

---

[119] SYDOW, Spencer Toth. O bem jurídico nos crimes informáticos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 113, pp. 193-212, mar./abr. 2015, p. 207. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=117946. Acesso em: 15 ago. 2021.

[120] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, pp. 189-190.

[121] SIEBER, Ulrich. Computer Crime and Criminal Information Law: New Trends in the International Risk and Information Society. *COMCRIME Study*. European Commission, 1998. Disponível em: https://www.law.tuwien.ac.at/sieber.pdf. Acesso em 28 set. 2021.

[122] ROSSINI, Augusto. *Informática, telemática e Direito penal*. São Paulo: Memória Jurídica, 2004.

[123] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021.

[124] Ibidem, p. 43.

No Código Penal pátrio, o delito tipificado no artigo 154-A (que, por excelência, diz respeito à integridade, confidencialidade e disponibilidade de informações) insere-se acertadamente no Título de Crimes contra a Liberdade Individual, bem jurídico tutelado de modo mediato.[125] De forma imediata, foram situados na Seção de crimes contra a inviolabilidade dos segredos. Contudo, na linha traçada pelos demais delitos contidos nessa Seção (divulgação de segredo e violação de segredo profissional), há enfoque limitado ao aspecto da confidencialidade dos dados, sendo também necessária a tutela a sua integridade e disponibilidade.

Dessa forma, revela maior proximidade a todos os prismas tutelados a proposta de o Mata y Martin,[126] para quem a liberdade constitucionalmente assegurada ao indivíduo se expande rumo à tecnologia informática. Dessa forma, os crimes informáticos consistem em uma violação aos diversos feixes que consubstanciam a liberdade de atuação no ambiente virtual, como violação à intimidade, domicílio, liberdade de expressão.

Mais especificamente, revela-se particularmente pertinente a expressão "autodeterminação informática".[127] Isso porque se permite conferir enfoque sobre o prisma da disponibilidade dos dados, aspecto usualmente olvidado pelas demais expressões. Ademais, reforça a concentração de todos os direitos sobre o titular, ao qual é facultado alterar, compartilhar, utilizar, ceder e inclusive destruir os dados. À luz da sociedade de risco atual, mostra-se imprescindível destacar a extensão das faculdades atribuídas ao titular, por um lado e, do outro lado da moeda, a responsabilidade advinda desse poder de disposição do bem.

Outrossim, o termo ora adotado elimina o desconforto erigido com a expressão "segurança informática", que traz um viés notoriamente protetivo e defensivo, porém olvida a vertente das liberdades inauguradas pelo ambiente virtual, dotada também de seu viés proativo em prol do livre desenvolvimento da personalidade – quer virtual, quer física – do indivíduo/usuário.

Por fim, essa denominação segue na linha do já consagrado direito fundamental à autodeterminação informativa, reconhecida por ordenamentos estrangeiros (como o alemão) e recentemente pelo Supremo Tribunal Federal. Corrobora, ainda, o entendimento conferido pelo poder constituinte derivado ao destacar a proteção de dados pessoais no meio digital como

---

[125] NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 3, 4. ed. Rio de Janeiro, Forense, 2019, p. 335.

[126] MATA y MARTIN, Ricardo M. Criminalidad Informática: uma introducción al cibercrimen. In: RUIZ MIGUEL, Carlos et al. *Temas de Direito da Informática e da Internet*. Coimbra: Coimbra, 2004, *apud* ROSSINI, Augusto. *Informática, telemática e Direito penal*. São Paulo: Memória Jurídica Editora, 2004, p. 132.

[127] Termo empregado por Brito, apesar de o autor preferir emprego da expressão segurança informática. BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 43.

direito fundamental explícito. A particularidade do bem jurídico consiste em seu especial enfoque: a tutela de dados no ambiente informático, dada suas peculiaridades inerentes à sociedade em rede e de risco, conferindo-se a necessária especificação atinente ao ambiente informático, que se torna o núcleo de tutela aos dados pessoais na atualidade – e, portanto, digno de tutela penal à luz do princípio da fragmentariedade. Por essas razões, adota-se na presente pesquisa o bem jurídico autodeterminação informática como aquele tutelado em se tratando de delitos informáticos próprios alusivos a bens jurídicos individuais.

A sociedade de risco e em rede, pela própria configuração das redes de comunicação, culmina com o individualismo como cultura predominante: as relações sociais podem ser acionadas ou desativadas a bel-prazer, são autoseletivas e estimulam a atuação individual: afinal, os próprios dispositivos são confeccionados para uso solitário.[128]

Outro reflexo da sociedade de risco são a perda da soberania estatal no ambiente informático e o consequente incremento da sensação de insegurança[129] – sendo muitas vezes a Internet vislumbrada como "terra de ninguém", sem leis ou regulamentação e permeada pela anonimidade: o medo se torna o código da atualidade.

Ocorre que a sensação de insegurança da sociedade de risco, potencializada pelo individualismo da sociedade de rede, sendo ambas vertentes componentes e definidoras do ambiente virtual, conduz ao já conhecido punitivismo penal, buscando-se incremento desenfreado de crimes e penas.[130]

Não obstante isso, o Direito Penal deve se pautar pelos princípios da ofensividade e da culpabilidade, reitores também no ambiente informático.[131] Assim, as estratégias de enfrentamento devem se afastar de mera demagogia punitiva, conferindo-se enfoque preventivo em duas das características reitoras da nova sociedade: na interconexão, que impõe uma atuação e regulamentação conjuntas dos países, e na individualização, a ensejar conscientização e educação dos usuários. Nesse contexto emerge uma necessidade de nova articulação entre criminologia, direito penal e política criminal: sem sua atuação conjunta e uniforme, haverá prevalência de leis penais rigorosas e ineficazes, impulsionadas pelo medo e individualismo dispostos na sociedade em rede.

---

[128] CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006, p. 24.
[129] BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. Tradução: Sebastião Nascimento. São Paulo: Editora 34, 2011, p. 13.
[130] GALÁN MUÑOZ, Alfonso. Mitos y realidades de la delincuencia informática. Un estudio sobre la reforma del Código Penal brasileño en materia de delitos informáticos, a la luz del Derecho penal Internacional. *Revista justiça e sistema criminal: modernas tendências do sistema criminal*, Curitiba, v. 1, n. 1, p. 57-98, jul./dez. 2009, p. 62. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=89162. Acesso em: 22 jul. 2021.
[131] Vide capítulo 2.4. (Princípios da intervenção mínima e culpabilidade).

2.3. (In)Disponibilidade do bem jurídico tutelado

A disponibilidade do bem jurídico diz respeito ao grau de interesse coletivo em sua preservação. Quando sua tutela se mostra relevante para a sociedade em geral, diz-se que um bem jurídico será indisponível, porquanto será protegido independentemente da vontade de seu titular.

Em regra, o bem jurídico será disponível, tendo em vista o direito geral de liberdade constitucionalmente assegurado (artigo 5º inciso II, da Constituição Federal), em prol do livre desenvolvimento da personalidade do ser humano. Assim, caso haja desinteresse na proteção por seu titular, não poderá o Estado se imiscuir, sob pena de se incorrer em indevido paternalismo penal. Dialoga, destarte, diretamente com o livre desenvolvimento da personalidade, entendendo-se que o indivíduo, como ser autônomo, é apto a tomar as próprias decisões, inclusive arriscando seu bem jurídico, em prol de seus objetivos particulares.

Por outro lado, pode-se traçar dois parâmetros principais que permitem concluir pela indisponibilidade de um bem jurídico. O primeiro deles consiste no grau de proximidade com o núcleo da dignidade da pessoa humana. Imaginando-se diversos círculos concêntricos em torno da dignidade humana, quanto mais próximo o bem jurídico se encontrar da própria natureza do ser humano, maior a indisponibilidade. Por esse motivo, entende-se que a vida, por ser inerente à existência humana, é bem jurídico indisponível. Do mesmo modo, veda-se a tortura ainda que mediante a anuência do indivíduo, por dizer respeito a violação à própria essência do ser humano.[132]

O segundo parâmetro consiste no caráter coletivo do bem jurídico tutelado. Quando se tratar de interesses difusos ou coletivos, invariavelmente se estará diante de bem jurídico indisponível, ante o manifesto interesse social em sua tutela. Por essa razão, são indisponíveis a proteção ao meio ambiente, sistema financeiro, administração pública e outros. A seu turno, todos os demais serão presumidamente de interesse privado e, portanto, disponíveis.

Por conseguinte, a discussão acerca da disponibilidade do bem jurídico dialoga diretamente com seu conceito constitucional, tal qual delineado por Roxin: como o bem jurídico se destina ao livre desenvolvimento de seu titular, calcado na dignidade humana, apenas será inviável sua renúncia ou exposição voluntária a riscos diante de interesse coletivo ulterior em preservá-lo.

---

[132] Ainda, a integridade física será dotada de caráter disponível caso se esteja diante de lesões corporais leves, porém será vedado o consentimento diante de lesões graves ou gravíssimas, porquanto mais próximas do cerne da dignidade humana.

Direcionando-se a temática sobre o bem jurídico tutelado no ambiente informático, pontua-se que, em regra, haverá sua disponibilidade por dizer respeito ao próprio indivíduo titular dos dados pessoais. Com efeito, como se depreende do Capítulo 1, bem como do Capítulo 2.2., discorreu-se acerca da proteção de dados como prisma de direitos e garantias individuais previstos no artigo 5º, notadamente a liberdade, a honra, privacidade, intimidade e inviolabilidade de dados. Todas essas manifestações apresentam caráter preponderantemente individual ligado ao livre desenvolvimento da personalidade de seu titular, que se torna protagonista em seu tratamento e disposição. Por conseguinte, o bem jurídico autodeterminação informática, delineado no Capítulo anterior, é essencialmente disponível.

A seu turno, não se olvida que a violação a dados pessoais tem aptidão a atingir interesses coletivos. Assim, merece destaque – apesar de fugir do escopo desta pesquisa – a vertente coletiva e difusa desse bem jurídico, visto sua tutela a toda a sociedade global, no que pertine à estabilidade de acesso à rede e à prestação de serviços públicos. Há notório caráter indisponível em se tratando de ataques de *Denial of Service* que levem a possível disrupção da rede.[133] É plenamente viável também a lesão direcionada a um órgão público, ou mesmo a um dos Poderes da República, conforme prevê o artigo 154-A, §5º, do Código Penal. Sob essa ótica transindividual, ganha maior relevância a vertente de proteção e segurança da rede, de modo a ser apropriado o tradicional bem jurídico alcunhado de segurança informática.

Para fins da presente pesquisa, voltada a bens jurídicos disponíveis, será conferido enfoque à autodeterminação informática, ou seja, à tutela sobre a confidencialidade, integridade e disponibilidade de dados pessoais sob a ótica individual e disponível.

Ainda, paralelamente se mostra pertinente o estudo conjugado de delitos patrimoniais no ambiente informático. Isso porque o patrimônio, direito fundamental de primeira dimensão, encontra-se entre os bens jurídicos que viabilizam o livre desenvolvimento individual. Não se trata de direitos constitutivos inerentes ao indivíduo, ínsitos à "existência jurídica de uma pessoa", de modo que se trata de instrumentos voltados à consecução de objetivos pessoais. Consistem em bens, por definição, transferíveis, alienáveis e disponíveis.[134]

Desse modo, o patrimônio estabelece uma relação dinâmica com o indivíduo, o qual pode dispô-lo livremente tendo em vista o livre desenvolvimento de sua personalidade. Essas ideias, no entendimento de Moccia, estão fortemente vinculadas à noção pessoal de patrimônio,

---

[133] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, pp. 170-171.

[134] KINDHÄUSER, Urs; CARO JOHN, José Antonio; GARCÍA CAVERO, Percy. *Estudios de derecho penal patrimonial.* Lima: Grijley, 2002, pp. 31-32. Disponível em: http://201.23.85.222/biblioteca/index.asp?codigo_sophia=72303. Acesso em: 20 mai. 2018.

o qual se apresenta como o conjunto de bens e relações úteis para o desenvolvimento do indivíduo, dotados de valor econômico. Uma ofensa ao patrimônio se manifesta com a limitação da potencialidade econômica apta a macular as finalidades pessoais do indivíduo.[135] Isso porque, como a disposição do patrimônio não diz respeito à essência da dignidade do ser humano, direciona-se, em verdade, a promovê-la ao reconhecer a autonomia do ser humano em sua destinação.

Nesse contexto, dados os contornos próprios dos crimes praticados no ambiente informático, torna-se viável a conjugação dogmática do estudo de bens jurídicos disponíveis nesse ambiente: a autodeterminação informática e o patrimônio. Por outro lado, como se pretende demonstrar, haverá nuances particularmente aplicáveis a cada qual, considerando-se que apenas o primeiro é insubsistente fora da seara informática.

2.4. Princípios da intervenção mínima e culpabilidade nos crimes informáticos

Ao se defender a criação de um novo bem jurídico, também é imprescindível delimitar seus contornos, com vistas a evitar sua exacerbada expansão, contrariando os ditames do Estado Democrático de Direito. Com efeito, conforme Da Ponte, a política criminal como materialização do Direito Penal exerce uma função dúplice: promove auxílio ao combate à criminalidade em defesa aos valores sociais mais comezinhos e, simultaneamente, traça um modelo de sistema a ser seguido.[136] Em um sistema punitivo aberto, que observe aos ditames democráticos, a política criminal deve se submeter aos princípios penais garantistas decorrentes expressa ou implicitamente da Constituição Federal.

O princípio da legalidade (artigo 5º, inciso II, da Constituição Federal) impõe limites à criminalização penal, que deverá ser prévia, escrita, taxativa e determinada. Contudo, por si, não obsta a criação de tipos penais iníquos, que não firam interesses fundamentais ou penas desproporcionais. Destarte, a intervenção mínima exsurge como princípio constitucional implícito, derivado da legalidade, a fim de restringir o arbítrio do legislador no tocante ao conteúdo das normas penais.[137]

Conforme posição doutrinariamente predominante, preconiza-se que a criminalização de certa conduta apenas é legítima caso seja imprescindível para a proteção de bens jurídicos

---

[135] MOCCIA, Sergio. *El derecho penal entre ser y valor: función de la pena y sistemática teleológica.* Buenos Aires: Julio César Faira, 2003, pp. 275-276.
[136] DA PONTE, Antonio Carlos. *Crimes eleitorais*. São Paulo: Saraiva, 2008, pp. 178-179.
[137] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte Geral.* 19. ed. São Paulo: Saraiva, 2012, p. 53.

contra lesões ou, ao menos, colocação em perigo. Emana assim a noção de subsidiariedade do Direito Penal, que apenas deve incidir caso os demais ramos jurídicos sejam ineficientes para a tutela (*ultima ratio*).[138] Logo, não basta a mera violação a bem jurídico para justificar a incidência penal: sua intervenção deverá ser aquela absolutamente indispensável para o livre desenvolvimento do indivíduo em sociedade.

Do princípio da intervenção mínima também deflui o princípio da fragmentariedade, vale dizer, o bem jurídico não é protegido *in totum* pela esfera penal: seleciona-se apenas seu fragmento, sua fração essencial para a vida em sociedade. Destarte, apenas se sancionam os "ataques mais graves aos mais caros valores sociais."[139]

Ainda, é forçoso reconhecer a intrínseca relação traçada com o princípio da ofensividade, segundo o qual a intervenção estatal apenas se justifica mediante uma efetiva exposição a perigo ou dano ao bem jurídico tutelado, conceito sintetizado pelo brocardo latino *nulla poena sine iniuria*.[140]

Em sua globalidade, verifica-se uma função dúplice da intervenção mínima: orientadora ao legislador na elaboração de normas incriminadoras abstratas e, paralelamente, interpretativa ao operador do direito, excluindo-se condutas *in concreto* da incidência penal.[141] A inobservância a esse princípio conduz essencialmente a duas consequências. A primeira consiste na violação ao direito ao livre desenvolvimento da personalidade humana – e, de modo reflexo, à dignidade humana –, tendo em vista que o exercício do *ius puniendi* estatal em um Estado Democrático de Direito deve se circunscrever apenas ao necessário para a pacífica vida em sociedade.

A segunda consequência, de viés prático, é o esvaziamento da finalidade preventiva da norma penal, visto que sua ampla abrangência conduz ao declínio de seu aspecto intimidatório (prevenção geral negativa), ou mesmo de reforço sobre a confiança da norma (prevenção geral positiva). Isso porque há um esvaziamento da mensagem normativa transmitida pela norma penal, decorrente de sua erosão perante a sociedade. É o que Carnelutti alcunhou de "inflação legislativa", gerando desvalorização comparável à inflação monetária.[142]

Paralelamente à intervenção mínima, o princípio da culpabilidade apresenta particular relevância aos crimes informáticos. A expressão "culpabilidade" é polissêmica na seara penal,

---

[138] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, p. 66.
[139] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, p. 67.
[140] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte Geral.* 19. ed. São Paulo: Saraiva, 2012, p. 61.
[141] Ibidem, p. 62.
[142] LUISI, Luiz. *Os princípios constitucionais penais*. Porto Alegre: Sérgio Antônio Fabris, 1991, pp. 26-28.

podendo ser subdividida em três acepções principais: a) noção de responsabilidade subjetiva, impondo-se que uma conduta apenas será penalmente relevante se for praticada ao menos culposamente; b) como terceiro elemento da teoria tripartite do crime, vinculada ao juízo de reprovabilidade do autor; c) proporcionalidade na dosimetria da pena, de modo que esta deverá refletir o grau de censurabilidade da ação, materializada no ordenamento pátrio no artigo 59 do Código Penal.[143]

A repercussão do princípio da intervenção mínima sobre os crimes informáticos se traduz inicialmente na conformação do bem jurídico próprio do ambiente virtual. Como visto, o direito fundamental à autodeterminação informativa é apto a abarcar dados pessoais obtidos e armazenados também em meios físicos. No entanto, as lesões de maior gravidade ocorrem na seara informática, dada sua potencial perenidade de armazenamento, instantaneidade e seu âmbito global. Soma-se a isso a elevada e crescente interdependência dos indivíduos quanto a informações virtualmente armazenadas, frequentemente de maior relevo quando comparadas a bens materiais. Assim, identifica-se que o núcleo essencial para a vida em sociedade no tocante à tutela de dados pessoais se circunscreve ao ambiente informatizado. Por essa razão, sob a ótica penal mostra-se desnecessária a criação de novos tipos penais e bens jurídicos para a proteção a dados pessoais armazenados fisicamente, porquanto já suficientemente tutelados pelo ordenamento.

O princípio da intervenção mínima também se desdobra, na seara virtual, em identificar qual a forma mais eficiente de coibir o ato danoso antes de promover a elaboração de tipos penais. Por esse motivo, é devida redobrada cautela na criação de bens jurídicos informáticos difusos dignos de tutela penal, em observância ao princípio da ofensividade penal: por se tratar de bens imateriais, sem efetiva concretude, mostra-se árdua tarefa a mensuração dos danos causados. Em verdade, frequentemente são limitados a delitos de perigo abstrato, cuja constitucionalidade tem sido questionada com a forte tendência de expansão penal. Dessa forma, entende-se que, de modo a frear uma excessiva e indevida expansão do Direito Penal, fato a qual chamam atenção Silva Sánchez e Morán, deve-se manter, ao menos por ora, a tutela de crimes propriamente informáticos sob a ótica individual, quer se refiram a pessoa de direito público ou privado, física ou jurídica.[144]

---

[143] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, pp. 71-72.

[144] Cf. SILVA SÁNCHEZ, Jesús-María; MORÁN, Ángel José Sanz. *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*. Madrid: Civitas, 2001. Isso porque há tutela suficiente conferida pelos crimes impropriamente informáticos sob a ótica difusa, de modo que uma violação a dados e dispositivos informáticos é apta a configurar crime ambiental, crime contra as relações de consumo e outros.

Por fim, a partir do prisma tripartite de proteção delineado na Convenção de Budapeste de integridade-confidencialidade-disponibilidade, confere-se concretude suficiente ao bem jurídico individual consistente na autodeterminação informática, em observância ao princípio da legalidade, sobretudo no tocante à precisão de seu conteúdo (*nulla poena sine lege certa*). Desse modo, não se visa a coibir a punição de atos preparatórios ou de condutas de perigo abstrato, mas de efetivas lesões, tratando-se de delito material. [145]

Voltando-se à análise do bem jurídico autodeterminação informática e, portanto, sob a ótica individual, verifica-se também que o princípio da intervenção mínima foi violado com a elaboração do artigo 154-A do Código Penal, promulgado às pressas em 2012 após episódios de mácula à privacidade da atriz Carolina Dieckmann. Se, por um lado, atualmente se faz necessária a tutela penal da autodeterminação informática, por outro, impunha-se um escrutínio técnico prévio para a criação de regras atinentes à responsabilidade civil e administrativa, o que foi feito posterior e tardiamente, apenas a partir de 2014. No entanto, partiu-se da lei penal para depois se cogitar de outros ramos jurídicos.

No tocante aos crimes patrimoniais (incluídos aqueles praticados no ambiente informático), o Pacote Anticrime trouxe uma alteração relevante em observância ao princípio da intervenção mínima: estabeleceu a ação penal pública condicionada à representação para o delito de estelionato, o que se mostra em conformidade com a natureza disponível do bem tutelado. Ocorre que se deixou de aplicá-la sobre o delito de furto, na contramão de um emprego coerente do princípio. Particularmente no tocante aos crimes patrimoniais informáticos, houve violação aos princípios da culpabilidade e intervenção mínima com o advento da Lei n. 14.155/2021, que estabeleceu penas desproporcionalmente elevadas para novos tipos penais patrimoniais criados.[146]

Como aponta Sydow, as soluções mais eficientes para a prevenção da prática de ilícitos (e até mesmo crimes) no ambiente virtual concentram-se em sua regulamentação pela via administrativa,[147] impondo-se obrigações a todos os agentes envolvidos: provedores de conteúdo, órgãos públicos, empresas, usuários. Discorre o autor que:

> É preciso verificar quais sujeitos envolver-se-ão na cadeia de ações e omissões para aperfeiçoar a violação e buscar preencher as brechas administrativas em cada degrau

[145] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021. Críticas são lançadas, no Capítulo 3.4.1.2., ao tipo penal previsto no artigo 154-A, §1º, do Código Penal, dado seu evidente caráter de perigo abstrato, em desacordo com o princípio da ofensividade. Trata-se de punição de atos preparatórios, de modo que não há efetiva lesão a bem jurídico autodeterminação informática.
[146] Capítulo 3.4.3. (Crimes informáticos patrimoniais impróprios).
[147] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, pp. 94-95.

> dentro do *iter*, sob pena de sepultar a eficiência da questão penal e, com isso, enaltecer o caráter de um Estado fraco e incapaz de executar as normas penais que cria.[148]

Como se demonstrará ao longo dos Capítulos seguintes, o papel desempenhado pelo usuário é, com frequência, direta ou indiretamente essencial para o desfecho danoso de práticas delitivas alusivas a bens jurídicos individuais, quer se trate do patrimônio, quer da autodeterminação informática. Assim, de pouca valia será um Direito Penal que desconsidere esse elemento no momento de elaboração e aplicação de normas penais, abstendo-se da adoção de medidas extrapenais de controle.

Ainda, nessa hipótese restará configurada a violação ao princípio da intervenção mínima, porquanto transbordará a repercussão penal necessária para a convivência pacífica em sociedade: o usuário, como protagonista do tratamento dispensado a seus dados informáticos em prol do livre desenvolvimento de sua personalidade, assume um papel ativo que também repercute em menor incidência penal. Do mesmo modo, haverá inobservância ao princípio da culpabilidade, sob a vertente de censurabilidade da ação, porquanto a contribuição da vítima sobre o resultado danoso mitiga a gravidade concreta do caso e, por conseguinte, deve repercutir sobre a sanção do agente.[149]

Essas considerações, que consistem no cerne da presente pesquisa, são aprofundadas quando do estudo da vitimodogmática no ambiente virtual (Capítulo 3), bem como com a construção funcionalista dos crimes informáticos (Capítulo 4).

---

[148] Ibidem, p. 95.

[149] Quanto ao ponto, ainda, observa-se a insuficiência do artigo 59 do Código Penal por ser vedada a redução da pena-base aquém do patamar mínimo legal fixado para o tipo penal.

3. CRIMES INFORMÁTICOS PRÓPRIOS E IMPRÓPRIOS

Traçou-se até o momento o panorama acerca da relevância da tutela constitucional dos crimes informáticos. O fundamento constitucional da proteção de dados pessoais, inicialmente sob seu viés protetivo-passivo, desenvolve um aspecto positivo-ativo, em que seu titular passa a ter disponibilidade plena sobre seu direito. Materializou-se na seara informática o cariz constitucional do livre desenvolvimento do indivíduo, vislumbrado como ser racional e livre, conforme preceitua a própria raiz da dignidade humana.

Por essa razão, a partir da teoria constitucionalista, traçou-se o bem jurídico-penal particularmente tutelado no ambiente informático: a autodeterminação informática, por meio do qual se realça a liberdade individual e a vertente liberal da Constituição, reverberando sobre os princípios penais da culpabilidade e da intervenção mínima.

Neste Capítulo, busca-se delinear os principais elementos para uma adequada leitura penal dos delitos praticados no meio informático. São expostos conceitos essenciais para a compreensão dos delitos informáticos, trazendo-se enfoque para as principais condutas lesivas a interesses jurídicamente tutelados, que podem ser sintetizados por meio de *malwares* e fraudes.

A partir de uma proposta de classificação, confere-se destaque ao estudo dos delitos informáticos atinentes a bens jurídico-penais indivíduais e disponíveis, em que há preponderância do aspecto do livre desenvolvimento do indivíduo: a autodeterminação informática e o patrimônio. Traçam-se, com isso, os pressupostos para compreensão do papel autorresponsável do usuário no ambiente informático e sua repercussão penal sobre a conduta do agente.

3.2.Definições informáticas

A Internet, constantemente aprimorada por diversos atores[150], teve sua inauguração em nível global em 1992, recebendo instantaneamente inúmeros adeptos em razão de sua

[150] O surgimento da Internet foi calculado e planejado, não sendo mera consequência fortuita de um projeto militar, mas sim de uma missão de cientistas em revolucionar a comunicação computadorizada. Um dos programas, a ARPANET, almejava o compartilhamento de recursos e informações online a tempo real, evitando-se eventual extravio de informação decorrente da destruição de seu suporte físico. Todos os desenvolvimentos-chave, como rede de proteção de dados e o protocolo IP foram promovidos por meio de instituições governamentais, grandes universidades e centros de pesquisa. Isso porque se tratava de tecnologia muito arrojada e custosa para a assunção dos riscos por entidades privadas. Por outro lado, Desde seu início, houve grande abertura na arquitetura da Internet: os próprios usuários passaram a ser tornar produtores da nova tecnologia e a moldar a rede. (CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006, pp. 19-27).

praticidade.[151] Paralelamente à sua imediata e progressiva utilidade no cotidiano, emergiram riscos nesse novo ambiente, materializados por novas práticas delitivas ou pelo aprimoramento de sua execução. Trata-se de mais um reflexo da sociedade de risco atual, sendo a inter-relação entre Direito Penal e Informática uma de suas principais vertentes.[152]

A compreensão das consequências jurídico-penais da sociedade em rede perpassa, portanto, pela interdisciplinariedade traçada com a informática, de modo que se torna essencial sedimentar conceitos-chave para a compreensão dos novos fenômenos delitivos. Para tanto, serão delineadas definições aptas a ser empregadas nas ciências criminais, considerando-se a carência de leis penais que realizem esse escrutínio.

Conforme Vianna e Machado, "uma informação é toda representação que um sujeito (*res cogitans*) faz de um objeto (*res cogitata*)".[153] No ambiente informático a linguagem da informação se baseia na presença ou ausência de corrente elétrica.[154]

De se notar que os dados são, simplesmente, "informações representadas de uma forma processável pelo computador".[155] Em uma comparação lastreada na comunicação, os dados consistem em uma linguagem própria do ambiente informático, submetida a um processo de tradução pelo dispositivo informático para a linguagem humana.

Um dispositivo informático, também denominado sistema computacional, é um conjunto de ferramentas apto a processar dados de maneira automatizada, ou seja, a efetuar comandos sem consecutiva intervenção humana. Essas ferramentas podem ser subdivididas em seu suporte físico e digital. Aquele, denominado *hardware*, se refere aos objetos materiais desenhados para receber as instruções humanas e exibir seus resultados. Em um *notebook*, o *hardware* é composto pelo disco rígido, processador, teclado, *HD* e outros. A seu turno, o suporte virtual consiste no software, ou seja, uma série de programas - conjunto de instruções direcionadas a um dispositivo informático para a resolução de uma tarefa específica.[156] O

---

[151] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 28.

[152] GALÁN MUÑOZ, Alfonso. Mitos y realidades de la delincuencia informática. Un estudio sobre la reforma del Código Penal brasileño en materia de delitos informáticos, a la luz del Derecho penal Internacional. *Revista justiça e sistema criminal: modernas tendências do sistema criminal*, Curitiba, v. 1, n. 1, p. 57-98, jul./dez. 2009, p. 60. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=89162. Acesso em: 22 jul. 2021.

[153] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 16.

[154] Assim, a forma mais eficiente de sua representação consiste em um sistema binário: 0 indica ausência de corrente, enquanto 1 indica sua presença. A partir desse sistema, efetua-se uma correlação entre caracteres, números, imagens e símbolos e uma representação lastreada em sequências binárias. Cada dígito binário é denominado bit, sendo necessário um conjunto de oito deles (*byte*) para se exprimir um caractere (VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, pp. 17-18).

[155] Ibidem, p. 19.

[156] Ibidem, p.23.

software é composto pelo sistema operacional e todos os demais programas destinados a executar funções específicas.

Os dispositivos informáticos podem estar interconectados em uma rede local (limitada a certa área), interna (intranet, muito utilizada em empresas, entre funcionários) ou global, denominada Internet, a qual permite interligação entre todos os dispositivos do mundo. Sydow apresenta três características essenciais da Internet: uma interligação entre redes, escala global e identidade de linguagem.

Dentro da Internet acessível por dispositivos usuais situa-se a *deep web*, parcela não indexada da rede. Deve-se ponderar que, predominantemente, a *deep web* é composta por atividades legais, tais como armazenamento de conteúdos de websites, dados de usuários, empresas programas e aplicativos, sendo acessada, por exemplo, mediante etapas de verificação de autorização (como login e senha).

Por outro lado, no interior da *deep web* pode ser localizada a *darkweb*, esta sim destinada à prática de ilícitos, em razão da potencialização da anonimidade. Para acesso à *darkweb* é necessária a instalação de um navegador próprio, denominado TOR (acrônimo de *The Onion Router*, em razão das diversas camadas que apresenta no tráfego de informações criptografadas).[157]

Dispositivos informáticos apresentam mecanismos de segurança, ou seja, *hardwares*[158] e/ou softwares destinados a assegurar a integridade, confidencialidade e disponibilidade dos dados e do próprio dispositivo. Um dos principais mecanismos de segurança é o *firewall* (em inglês, parede corta-fogo), cuja principal função é filtrar o acesso ao dispositivo com base em uma série de instruções, de modo a bloquear conexões não autorizadas e, portanto, potencialmente nocivas.[159] Assim, o *firewall* controla o tráfego de rede.

Ademais, essencial mecanismo de segurança é o *antimalware*, programa destinado para prevenir, rastrear e destruir *malwares* instalados no computador. Softwares mais conhecidos são os antivírus e *antispyware*.

---

[157] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 59.

[158] Em regra, para uso diário e doméstico, o *firewall* é apenas um software. Porém, em redes de grande porte e empresas que necessitam de especial proteção a seus dispositivos, há equipamentos específicos (*hardwares) destinados à segurança da rede.*

[159] XIE, Huagang; WANG, Xinran; LIU, Jiangxia. *Malware analysis system.* U.S. Patent n. 9,047,441, Publicação: 02 mai. 2011, Concessão: 02 jun. 2015, p. 12. Disponível em: https://patents.google.com/patent/US9047441B2/en. Acesso em: 29 set. 2021.

3.2.1. Condutas lesivas no ambiente informático

Na seara informática, pode-se dizer que o desenvolvimento legislativo brasileiro foi extremamente tardio – iniciando-se em 2012, com leis criminais, em subversão ao princípio da subsidiariedade. Se não bastasse, muitas condutas lesivas não foram abarcadas pelos tipos penais criados, e tampouco o são com o advento da Lei n. 14.155/2021.

A seguir, busca-se elencar uma série de condutas praticadas no ambiente virtual dignas de ponderação sobre o atual enquadramento típico ou mesmo sobre a (des) necessidade de elaboração de novas leis penais, à luz do princípio da intervenção mínima.

3.2.1.1. *Phishing* e Engenharia social

O elo mais vulnerável de todo mecanismo de segurança no ambiente informático é o ser humano. Com efeito, a maioria dos acessos indevidos a dispositivos informáticos é ocasionada, direta ou indiretamente, por uma conduta humana. Isso porque muitos creem que os mecanismos de segurança, por si, fornecem adequada proteção, sujeitando-se a uma ilusão de segurança.[160] Ademais, em razão do ritmo de vida acelerado da população, que levam a uma escassez de tempo e desgaste mental, frequentemente são tomadas decisões após pouca reflexão, de forma a gerar resposta automáticas inclusive em aspectos relevantes ao longo da vida.[161] Nesse contexto, tornam-se essenciais características individuais como a ganância, descuido ou ignorância dos usuários.

O *phishing*[162] é um dos principais mecanismos que busca explorar essa fragilidade. Trata-se de qualquer modalidade de engodo ou fraude por meios digitais – podendo, frequentemente, envolver telefonemas, mensagens, e-mails – com vistas a obter informações dos destinatários. Todo ataque de *phishing* apresenta três elementos: a) emprego de instrumentos informáticos (e-mail, redes sociais, páginas de Internet) ou de telecomunicação; b) fraude perante o usuário, mediante o qual o agente ou anúncio aparenta ser indivíduo ou instituição confiável; c) objetivo de obtenção de informações privadas, notadamente com vistas a vantagens financeiras.

---

[160] MITNICK, Kevin D.; SIMON, William L. *A arte de enganar*. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003, p. 15.
[161] Ibidem, p. 106.
[162] O termo "phishing" deriva da conjugação das palavras inglesas "fishing" e "phreaking". Trata-se de fishing ("pesca"), porquanto o agente oferece uma "isca" (mediante fraude) ao usuário, que será fisgado caso forneça informações pessoais. O termo "pheraking" (entusiasta), a seu turno, deriva da prática corriqueira de experimentos com sistemas de telecomunicação nos anos 1950 com objetivo de compreender seu funcionamento.

Com o avanço de sites de relacionamento e redes sociais, tornou-se tarefa extremamente simples a obtenção de informações acerca de usuários, de modo que os *phishers* (agentes que praticam *phishing),* em seu poder, conferem maior credibilidade a suas fraudes, o que favorece a proliferação de ataques. Aliás, a própria natureza social humana leva o indivíduo a crer que não será enganado, a menos que tenha um motivo plausível para crer no contrário. Ou seja: confere-se, em regra, o "benefício da dúvida."[163]

Conforme apontam Jesus e Milagre, a prática de *phishing* apresenta algumas vertentes.[164] Primeiramente, verifica-se com a prática de engenharia social, hipótese em que é prescindível conhecimento técnico prévio dos agentes, porquanto basta a mera persuasão do usuário para transferência de valores ou informações.

Com efeito, ainda na atualidade, o mecanismo mais simples de obtenção de informações consiste em perguntar diretamente à vítima, induzindo-a a fornecê-las por meios fraudulentos. Há diversos esquemas, frequentemente denominados *honey pots* (que atraem pessoas distraídas ou ingênuas), como o enriquecimento rápido (*get rich quick*) ao oferecer recebimento rápido de valores por suposta herança, prêmio em sorteio. Há também *gold brick schemes*, em que se oferece um produto a preço bem inferior ao de mercado (como em falsos leilões), porém o comprador recebe mercadoria falsificada, de qualidade inferior à anunciada, ou sequer recebe algo.[165] Existem ainda anúncios de tragédias, com supostos indivíduos que necessitam de valores para um tratamento médico ou instituições filantrópicas que solicitam doações.

Surgem ainda esquemas de aplicativos e sites de relacionamento (como o Tinder), em que a pessoa simula interesse por um relacionamento amoroso, apenas para obter dados e valores da vítima.

Outras formas de *phishing* mediante engenharia social apelam aos sentimentos da vítima, gerando comoção ou receio de ostentar dívidas. Há sites que aparentam ser reais, porém apresentam nome de domínio falso, trocando-se algum caractere, imitando instituições confiáveis para cobranças, necessidade de confirmação de senhas ou problemas no cadastro.[166] São comuns envios de e-mails e telefonemas por supostas ONGs, órgãos públicos, instituições

---

[163] MITNICK, Kevin D.; SIMON, William L. *A arte de enganar*. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003, p. 46.
[164] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016, pp. 145-146.
[165] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, p. 112.
[166] Exemplo com o Paypal: enquanto o site verdadeiro é " www.paypal.com ", o site falso altera uma letra, tornando-se "www.paypai.com". MITNICK, Kevin D.; SIMON, William L. *Op. cit.*, pp. 87-88.

financeiras que anunciam a existência de dívidas. Diante disso, o usuário fornece seus dados, ou mesmo efetua o pagamento de falsos boletos.

Sydow traz seis elementos frequentemente presentes em golpes mediante engenharia social: a) reciprocidade, em que se oferece algo em troca pelos dados ou valores; b) compromisso moral, como fatores apelativos a fome e doenças; c) prova social, revelando ser prática frequente ou corriqueira a conduta almejada; d) autoridade, como órgãos públicos e instituições financeiras; e) afinidade, trazendo sensação de familiaridade e sinceridade ao interlocutor; f) escassez ou oportunidade imperdível do produto ou serviço.[167]

Segunda modalidade de *phishing* consiste na inserção de malware no dispositivo informático do usuário, o qual voluntária ou involuntariamente executa um arquivo ou *link* malicioso em razão de fraude praticada pelo agente. Nessa hipótese, o malware desencadeado desativa mecanismos de segurança ou fornece dados para acesso ao dispositivo. Pode ser instalada uma *backdoor* (falha no sistema operacional que permita ingresso por terceiro), ou mesmo *worms*, que disparam e-mails a todos os contatos daquele usuário do dispositivo.

Por fim, o *phishing* também pode ser executado mediante inserção de *keylogger*, espécie de malware que acessa o dispositivo do usuário a fim de capturar todas as teclas digitadas e histórico de atividades.[168]

Para além do *phising*, outro instrumento que explora a ingenuidade ou fragilidade dos usuários são os ataques de força bruta (*password guessing*). Em razão da displicência quando da criação de senhas, frequentemente são utilizados padrões previsíveis, como datas de nascimento próprio ou de parentes, nomes e sobrenomes, ou mesmo padrões de fácil memorização, como "senha" e "1234".[169]

Como se vê, parcela significativa dos mecanismos de engodo exploram exclusivamente a ignorância, leviandade e inexperiência dos usuários. Porém, há diversos mecanismos que conjugam esses fatores com conhecimentos técnicos informáticos, resultando em condutas lesivas a seus titulares.

Em geral, indivíduos que apresentam excepcional conhecimento técnico sobre o ambiente informático e são capazes de superar mecanismos de segurança de dispositivos são denominados *hackers*. Essa expressão, contudo, apresenta conotação neutra, visto que hackers

---

[167] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, pp. 582-583.
[168] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 146.
[169] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 63.

podem ser dotados de finalidade legais e louváveis, posto que capazes de fornecer soluções ágeis a problemas no ambiente digital, inclusive evitando a invasão de dispositivos.

Por outro lado, sob a ótica negativa, o *hacker* é denominado *cracker*, o qual se dispõe a invadir computadores para a prática de objetivos lesivos, como deletar e substituir dados para ganho pessoal, sabotagem, vingança, ou mesmo prejudicar empresas e nações inteiras.[170]

Os crackers, em regra, desenvolvem e empregam *malwares* em suas condutas, consistentes em softwares maliciosos aptos a ingressar no dispositivo informático sem o consentimento do usuário e, frequentemente, sequer sem seu conhecimento. O denominador comum dos malwares consiste no ingresso sub-reptício no dispositivo e na potencialidade de gerar algum dano ao usuário. Apesar de sua vasta gama, em regra o usuário instala o malware involuntariamente, na crença de se tratar de algum programa ou link de sua utilidade. A seguir, serão abordados os principais *malwares* desenvolvidos por crackers, sem a pretensão de esgotá-los, considerando-se sua constante atualização.[171]

3.2.1.2. Espécies de *malwares*

Ramsomware é um *malware* que bloqueia o computador ou obsta o acesso do usuário a seus dados após criptografá-los ou subtraí-los, com o objetivo de requerer o pagamento de valores – geralmente em bitcoins ou outras criptomoedas – como condição de sua restituição.[172] É prática muito frequente em face de empresas e entidades públicas, aptos a desembolsar maiores quantias. No entanto, muitos são projetados para atingir *notebooks* e aparelhos celulares, inclusive mediante alteração da senha de acesso. Em regra, são mais eficientes e danosos os *ramsomwares* baseados em criptografia, posto que, apesar de não destruírem os dados, obstam seu acesso caso não seja fornecido código para descriptografia, inclusive após total remoção do *malware*.[173]

Enquanto o *ramsomware*, após sua inserção, revela-se ao usuário a fim de obter o pagamento do "resgate" pelos dados, os demais *malwares* costumam se ocultar no sistema informático, a fim de obter informações e causar danos desapercebidamente. Exemplo emblemático é o *spyware*, destinado a monitorar o comportamento dos usuários e obter

---

[170] SCHELL, Bernadette Hlubik; SCHELL, Bernadette; MARTIN, Clemens. *Webster's new world hacker dictionary*. Indianapolis: Wiley Publishing, 2006, p. 8.

[171] O emprego da expressão "vírus" tem sido utilizado de forma genérica para se referir aos *malwares*. Ocorre que, a rigor, apenas são denominados vírus os softwares que apresentam finalidade de replicação após se apropriarem de programas do dispositivo informático, destruindo, obtendo ou alterando dados.

[172] RICHARDSON, Ronny; NORTH, Max M. Ransomware: Evolution, mitigation and prevention. *International Management Review*, v. 13, n. 1, p. 10-21, 2017, p. 10.

[173] Ibidem, p. 10.

informações particulares, como padrões de navegação, dados pessoais, gravação de áudio, captura de tela (*screenlogger*), teclas digitadas (*keylogger*).[174] Uma característica distintiva dos *spywares* é o envio dos dados armazenados a um terceiro, normalmente o agente que os utiliza.[175]

Rootkits são uma espécie de *malware* que concede acesso e controle a nível administrativo sobre um sistema operacional. Com isso, rootkits são capazes de obter e alterar informações e programas do dispositivo sem qualquer conhecimento de seu titular.[176] Sua denominação "*root*" + "*kit*" (raiz + conjunto, pacote) desvelam seu método de funcionamento: acesso profundo, ao núcleo do sistema, mediante pacotes de software, frequentemente denominados Cavalos de Troia (aparentam ter utilidade, mas trazem em seu bojo algum *malware* de forma sub-reptícia).

Por outro lado, *rootkits* podem ser instalados voluntariamente pelos usuários com vistas a superar obstruções internas dos fabricantes, como ocorre em dispositivos iOS, em operação denominada *Jailbreak*.

Worms são *malwares* autoexecutáveis que, uma vez instalados, são aptos a se propagar através de uma rede de computadores sem qualquer interação do usuário. Assim, diferem dos vírus porquanto estes, embora também consistam em *malwares* replicáveis, necessitam se apropriar dos programas do computador para contaminação de outros.

Originalmente, os *worms* necessitavam de suportes físicos, como CDs e *pendrive* USB para serem inseridos. Contudo, atualmente estão presentes em diversos mecanismos, como websites e e-mails. Ademais, *worms* são imperceptíveis, pois abrem a *backdoor* (porta dos fundos dos computadores), sendo que frequentemente trazem consigo outros *malwares*, como ransomware. A infecção de outros dispositivos pode ocorrer ativamente (tanto a partir de uma lista de alvos pré-selecionados, como utilizar informações do próprio dispositivo infectado) como passivamente (por meio de contágio de computadores que estabelecem alguma conexão com o dispositivo).[177]

---

[174] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 35.

[175] KIRDA, Engin *et al*. Behavior-based Spyware Detection. In: *Usenix Security Symposium*, pp. 273-288 of the Proceedings, 2006, p. 273. Disponível em: https://www.usenix.org/legacy/event/sec06/tech/full_papers/kirda/kirda_html/ . Acesso em 28 set. 2021.

[176] EMBLETON, Shawn et al. SMM rootkit: a new breed of OS independent malware. *Security and Communication Networks*, v. 6, n. 12, pp. 1590-1605, 2013, p. 1590.

[177] AZIZ, Ashar. *System and method of containing computer worms*. U.S. Patent n. 8,549,638, publicação 13 jun. 2005, concessão: 1 out. 2013. Disponível em: https://portal.unifiedpatents.com/patents/patent/US-8549638-B2. Acesso em: 28 set. 2021.

Botnet (rede de robôs ou rede de zumbis) não é propriamente um *malware*, mas uma rede de dispositivos infectada por *malwares* (que podem ser *worms*, *rootkits* e outros) voltados a submetê-los ao comando do *cracker* ("*botmaster*"). Com o controle remoto de todos os dispositivos, o *botmaster* é capaz de elaborar ataques mais danosos, como *phishing* em larga escala e *Denial of Service*, e com menores riscos de rastreamento em razão da anonimidade.[178] A *botnet* também é empregada na prática de pirataria e subtração de informações.

Como mencionado, a *botnet* é frequentemente utilizada em ataques de *Denial of Service*, direcionados a impedir usuários legítimos de acessar certo endereço na rede. Há dois principais métodos de *DoS*: envio direto ao provedor de *malwares* com vistas a confundir o protocolo ou o programa, ou prejudicar a conectividade do provedor, reduzindo a extensão da banda, capacidade de processamento ou esgotando os recursos como memória, CPU. O *Distributed Denial of Service*, prática mais notória, efetua ataque de negação de serviço por congestionamento.[179] Em regra são ataques praticados pela botnet, de modo que o volume de acessos simultâneos leva a uma sobrecarga do sistema, ocasionando lentidão ou total queda.[180]

De grande relevância atualmente também são as injeções SQL. Um procedimento SQL é uma solicitação de consulta em banco de dados, normalmente atrelado à digitação de usuário e senha em *website*s e *Internet Banking*. Ocorre que muitos sites não verificam se sua entrada guarda correlação com o dado esperado, de modo que um *cracker* por inserir suas próprias solicitações no banco de dados. Assim, obtém acesso e controle às informações armazenadas.

Além de *malwares*, pode-se citar o *spam* e *adware* como atividades invasivas e incômodas ao usuário.[181] Apesar de frequentemente não visarem a causar dano – caso sejam fraudulentas, estaremos diante de *phishing* –, podem levar à perturbação de uso do dispositivo – com distrações, congestionamento da rede –, bem como a excessivo dispêndio de tempo.

---

[178] FEILY, Maryam; SHAHRESTANI, Alireza; RAMADASS, Sureswaran. A survey of botnet and botnet detection. In: *2009 Third International Conference on Emerging Security Information, Systems and Technologies.* IEEE, p. 268-273, 2009, p. 268. Disponível em: http://www.itk.ilstu.edu/faculty/ytang/botnet/3%202009-A%20Survey%20of%20Botnet%20and%20Botnet%20Detection.pdf. Acesso em: 28 set. 2021.

[179] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 37

[180] ZARGAR, Saman Taghavi; JOSHI, James; TIPPER, David. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, v. 15, n. 4, p. 2046-2069, 2013, p. 2046.

[181] *Spamming* é o ato de enviar mensagens em massa não solicitadas, com intuito comercial, eleitoral ou mesmo pornográfico. Trata-se de técnica simples para promoção do produto ou serviço, normalmente por meio de e-mails. Por essa razão, aliás, muitos provedores de e-mail desenvolveram uma segunda caixa de entrada, destinada a filtrar e-mails considerados *spam*. A seu turno, *adware* consiste na publicidade excessiva constante de páginas da Internet, também voltadas a fins comerciais ou ao acesso a determinado *website*. Por meio de cookies e outros mecanismos, *adwares* coletam dados de navegação a fim de fornecer anúncios compatíveis com o interesse de cada usuário.

3.3. Nomenclatura e classificação dos crimes informáticos

A notoriedade e a especificidade de tratamento dispensadas aos crimes informáticos trazem à tona a indagação acerca do surgimento de um ramo autônomo, denominado Direito Penal Informático, conforme defendido por Sydow.[182] Isso porque não se está a falar simplesmente de novos tipos penais ou bens jurídicos, mas de uma sistemática de análise e interpretação dos institutos penais. Outros autores, como Crespo,[183] defendem que a dogmática penal tradicional é suficiente para a abordagem do tema, marcado por uma especialização dos institutos tradicionais.

Ao nosso sentir, a solução intermediária se revela mais profícua. O surgimento do ambiente informático e, com ele, de novos bens jurídicos, implica um constante repensar sobre a ciência dogmática penal, assim como feito quanto à criminologia.[184] Deve-se reconhecer, destarte, especificidades e aplicabilidade *sui generis* de institutos penais clássicos. Por outro lado, não se vislumbra autonomia científica bastante para a inauguração de uma nova ciência. A melhor solução consiste em uma adaptação da ciência penal vigente, reconhecendo-se a instantaneidade, ubiquidade e alta danosidade dos delitos informáticos na sociedade de risco.

Feita essa necessária observação, há múltiplas nomenclaturas empregadas em referência aos crimes praticados no meio virtual. A polissemia ecoa na esfera internacional, em que se faz alusão a expressões como "cybercrimes" (utilizada na Convenção de Budapeste), "computer crimes" (expressão classicamente empregada nos Estados Unidos), "netcrimes", "e-crimes", e outros. Em verbete português, são correntes as expressões "crimes virtuais", "crimes informáticos", "crimes digitais", "crimes cibernéticos", etc.

A escolha da nomenclatura deve levar em consideração a constante evolução tecnológica e alteração do ambiente virtual, renunciando-se à mera importação de termos tradicionalmente empregados no estrangeiro. Donde decorre a exclusão de termos demasiadamente restritivos, como "computer crimes" (alusivos apenas a computadores, mas olvidando-se demais dispositivos) e crimes digitais (lastreado em lógica binária, progressivamente se tornando superada pela computação quântica). Ainda, apesar de tradicionalmente vinculada a aspectos informáticos, o termo "cyber", proveniente do grego "governar", não faz alusão adequada ao bem jurídico ou ao objeto material. Assim, entende-se

---

[182] SYDOW, Spencer Toth. O bem jurídico nos crimes informáticos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 113, pp. 193-212, mar./abr. 2015, p. 245. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=117946. Acesso em: 15 ago. 2021.
[183] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011.
[184] Capítulo 4.2. (Criminologia e crimes informáticos).

que a expressão "crimes informáticos" é aquela mais abrangente e que melhor contempla o objeto do estudo criminal: a informática, que revela enfoque sobre as informações sob o viés tecnológico.

Tampouco há consenso quanto à classificação dos crimes informáticos, ou mesmo quanto às condutas subsumíveis sob esse espectro. De qualquer modo, vale ressaltar o vetusto – porém sempre contemporâneo – brocardo de que não existem classificações corretas ou equivocadas, mas úteis ou inúteis.

Para os fins propostos, uma classificação excessivamente minuciosa não se mostra contraproducente, sendo recomendável agrupar alguns delitos que merecem tutela penal semelhante.

Tradicionalmente, Klaus Tiedemann,[185] a partir de delitos econômicos, estabeleceu uma classificação tetrapartida sintetizada em: a) manipulações, direcionadas ao sistema de entrada ou saída de dados; b) espionagem; c) sabotagem, com a elisão de programas; d) furto de tempo, com uso indevido de *hardwares* por terceiros ou empregados.

Nos anos 90, Ulrich Sieber, catedrático da Universidade de Würzburg, em parecer para a Comissão Europeia,[186] discriminou os crimes informáticos em: 1. Violação à privacidade, com obtenção, armazenamento, transmissão e conexão de dados pessoais, que eram de pouca importância à época, respondendo por cerca de 1% dos crimes informáticos; 2. Crimes econômicos, principal enfoque adotado no século XX, respondendo pela maior proporção de delitos à época; 2.1. Hacking: invasão de sistema computacionais pelo simples prazer de superar medidas técnicas de segurança; 2.2. Espionagem: subtração de imensas quantidades de informações armazenadas em bancos de dados, como dados de pesquisas, endereços de clientes; 2.3. Pirataria de software e outras modalidades: mediante obtenção de *know-how* interno de uma companhia, com a produção de cópias não autorizadas; 2.4. Sabotagem e extorsão: imposição de danos físicos ou lógicos aptos a destruir os dados, que pode ser seguida de extorsão; 2.5. Fraudes, geralmente voltadas a bancos de dados e instituições financeiras; 3. Conteúdos ilegais e nocivos: violência, racismo, apologia ao crime; 4. Outros delitos, como ataques à vida (mediante manipulação de computadores de hospitais), crime organizado e guerras eletrônicas (ataques militares a sistemas informáticos inimigos).

---

[185] TIEDEMANN, Klaus. *Poder económico y delito*. Tradução: Amelia Mantilla Villegas. Barcelona: Ariel, 1985, pp. 122-129 *apud* CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 60.

[186] SIEBER, Ulrich. Computer Crime and Criminal Information Law: New Trends in the International Risk and Information Society. *COMCRIME Study*. European Commission, 1998. Disponível em: https://www.law.tuwien.ac.at/sieber.pdf. Acesso em 28 set. 2021, pp. 40-58.

Deve-se considerar o relevante valor dessas classificações ponderadas no século 20, de forte predominância de delitos econômicos. Não obstante isso, Briat[187] acrescentou um critério interessante em sua classificação, distinguindo delitos-meio, em que a informática é um instrumento para a prática delitiva, e demais delitos, em que elementos informáticos são alvo da conduta.

Na seara pátria, Greco Filho[188] efetua uma distinção abrangente, lastreada no bem jurídico afetado, de modo a distinguir crimes informáticos em: a) condutas perpetradas contra um sistema informático; b) condutas perpetradas contra outros bens jurídicos. Para Crespo, referida classificação mostra-se adequada, posto que sintética e apta a abarcar a mais ampla gama de delitos praticados no meio informático na atualidade.[189]

A objetividade e clareza desses conceitos tornam sua adoção popular, culminando com a distinção entre crimes informáticos próprios (que atingem o bem jurídico autodeterminação informática) e impróprios (que atingem os demais bens jurídicos).

Contudo, o refinamento das condutas informáticas, bem como as diferentes modalidades de atuação da vítima frente aos delitos impõe, com vistas a uma maior clareza de tratamento na presente pesquisa, um aprofundamento dentre as condutas ilícitas que atingem bens jurídicos tradicionais.

Posto isso, propõe-se uma classificação a partir da proposta de Crespo, lastreada em delitos informáticos próprios e impróprios, conferindo-se, porém, nuances nos termos sugeridos por Vianna e Machado:[190]

1. Delitos informáticos próprios: a proteção recai sobre o próprio bem jurídico informático,[191] ora entendido como a autodeterminação informática. Encontram-se tipificados na legislação pátria os seguintes delitos: invasão de dispositivo informático (art. 154-A, do Código Penal), produção, oferta, distribuição, venda ou difusão de dispositivo ou programas

---

[187] BRIAT, Martine. La fraude informatique: une approche de droit compare. *Révue de Droit Pénal et Criminologia*, Bruxelles, n. 4, 1985, p. 287 *apud* JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 52. Sua classificação pode ser subdividida em:1. Manipulação de dados ou programas com vistas à prática de delitos tradicionais; 2. Falsificação de dados e programas; 3. Destruição de dados e programas ou obstrução de sua utilização; 4. Divulgação, uso ou reprodução indevida de dados e programas; 5. Uso não autorizado de sistemas de informática; 6. acesso não autorizado a sistemas de informática.

[188] Algumas observações sobre o direito penal e a Internet. *Boletim IBCCRIM*, São Paulo, edição especial, ano 8, n. 95, 2000 *apud* CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 62.

[189] CRESPO, Marcelo Xavier de Freitas. *Op. cit.*, p. 63.

[190] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 32.

[191] Ibidem, p. 32.

com o intuito de invasão de dispositivo informático (Artigo 154-B, do Código Penal), interceptação telemática sem autorização judicial (artigo 10, da Lei n. 9.296/1996);

2. Delitos informáticos impróprios *lato sensu*: com a conduta visa-se a atingir bem jurídico diverso, dentre os tradicionalmente existentes, nos termos propostos por Crespo; [192]

2.1. Delitos informáticos impróprios *stricto sensu*: o computador ou sistema informatizado é utilizado como instrumento para a prática delitiva, contudo não há qualquer lesão ao bem jurídico informático em si.[193] Há uma vasta gama de delitos perpetrados por meios informáticos, tais como: delitos contra a honra, racismo, ameaça, induzimento, instigação ou auxílio ao suicídio, apologia ao crime, tráfico de drogas. É válido acrescentar os crimes de inserção de dados falsos em sistema de informações (artigo 313-A, do Código Penal) e modificação ou alteração não autorizada de sistema de informações (artigo 313-B, do Código Penal). Para os fins ora propostos, merecem especial destaque os delitos de estelionato (artigo 171, *caput*) - induzindo a vítima à entrega de valores e bens – e fraude eletrônica (artigo 171, §2º-A) – induzindo o usuário ao fornecimento de dados sensíveis, como senhas bancárias –, mediante prática de engenharia social e *phishing*;

2.2. Delitos informáticos mistos: a mesma norma penal tutela simultaneamente a autodeterminação informática e bem jurídico diverso, erigindo um tipo penal autônomo dada sua especial importância.[194] Isso porque a elementar típica contém em sua descrição alguma violação informática – normalmente materializando-se como instrumento para a prática delitiva, em uma relação comparável a um crime meio (em referência ao princípio da consunção). Trata-se, portanto, de crimes complexos, os quais devem ser elencados como delitos informáticos impróprios pois pressupõem especial fim de agir do agente, sempre direcionado a bem jurídico diverso. Principal exemplo citado por Vianna e Machado consiste no artigo 72, inciso I, do Código Eleitoral,[195] em caso de delito consumado, ou o artigo 67, inciso VII, da Lei n. 9.100/95, na hipótese de crime tentado.[196] Ademais, enquadra-se como crime misto o delito previsto no artigo 359-N, do Código Penal, porquanto visa tutelar o

---

[192] Cf. CRESPO, Marcelo Xavier de Freitas. *Op. cit.*

[193] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 30.

[194] Ibidem, p. 35.

[195] Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos.

[196] Art. 67. Constitui crime eleitoral: (...) VII – obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos. Conforme expõem Vianna e Machado, a modalidade consumada desse delito foi tacitamente revogada pelo artigo 72, do Código Eleitoral, o que não ocorreu com a tentativa, devendo prevalecer o princípio da especialidade como ferramenta para resolução do conflito aparente de normas. (VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, 35).

funcionamento das instituições democráticas no processo eleitoral e, simultaneamente, a integridade do sistema eletrônico do Tribunal Superior Eleitoral.[197] Trata-se, por fim, do novo delito de furto qualificado mediante fraude por meio de dispositivo informático (artigo 155, §4º-B, do Código Penal), que encerra em seu tipo penal o emprego de dispositivo informático – violando-se a integridade, confidencialidade e disponibilidade de dados do titular – para a obtenção de vantagem patrimonial;

2.3. Delitos informáticos mediatos ou indiretos: para a prática do delito-fim, atinente a bem jurídico diverso, pratica-se delito-meio tipificado como delito informático próprio. Diferentemente dos delitos mistos, não há tutela imediata ao bem jurídico autodeterminação informática, incidindo-se o princípio da consunção. Nas palavras de Vianna e Machado: "O crime-fim será classificado como informático mediato ou indireto quando, pela aplicação do princípio da consunção, um crime-meio informático não for punido em razão da sua consumação".[198] Como exemplo, pode-se citar a invasão de dispositivo informático de uma ex-companheira para a obtenção de cenas de sexo nele gravadas, com a posterior transmissão sem autorização do vídeo para terceiros. Nessa hipótese, o delito informático próprio, tipificado no artigo 154-A, do Código Penal, é absorvido pelo delito fim, divulgação de cena de sexo (artigo 218-C, do Código Penal).

A distinção entre delitos informáticos mistos e mediatos tende a se esvaziar com o surgimento de novos tipos penais informáticos (como o caso do furto mediante fraude por invasão de dispositivo informático), todavia, ainda se mostra relevante para viabilizar uma reflexão acerca da (des) necessidade de criação de novos delitos especificamente voltados ao ambiente virtual.

Convém ponderar que, a rigor estritamente técnico, os delitos impróprios *stricto sensu* não deveriam ser rotulados como informáticos, visto que o bem jurídico atingido não guarda relação com a inviolabilidade da informação automatizada. Ocorre que esse agrupamento se mostra relevante, posto que surgem desafios comuns aos delitos próprios e impróprios, de modo que o mesmo *modus operandi* virtual pode ser empregado para a prática de uma vasta gama de delitos. Esse fator é potencializado com a exposição massificada de particulares ao ambiente virtual.

---

[197] Art. 359-N. Impedir ou perturbar a eleição ou a aferição de seu resultado, mediante violação indevida de mecanismos de segurança do sistema eletrônico de votação estabelecido pela Justiça Eleitoral:Pena - reclusão, de 3 (três) a 6 (seis) anos, e multa.

[198] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 36.

Nessa linha, aponta Sydow: "o uso do meio ambiente *sui generis* é fator que agrava e aumenta a perspectiva da conduta seja porque encoraja a ação de um delinquente, traz sensação de impunidade e até mesmo viola um grande número de pessoas."[199]

Assim, diante da sociedade de risco, a compreensão dogmática, bem como criminológica dos delitos não pode ser dissociada dos instrumentos inerentes ao mundo digital. Vale dizer: há uma inter-relação entre todos os delitos perpetrados em meio digital sob a ótica das ciências criminais, o que impõe seu agrupamento para uma abordagem uniforme desse denominador comum.

Aliás, como se discorre no Capítulo 4.4. (Proposta de classificações das vítimas informáticas), referida realidade é evidenciada a partir dos perfis de vítimas traçados, que podem se mostrar suscetíveis do mesmo modo a delitos próprios e impróprios. Da mesma forma, sob uma perspectiva vitimodogmática, mostra-se relevante estabelecer parâmetros mínimos de cautelas atribuídas às vítimas no que tange a todos os crimes que envolvem meios informáticos, notadamente quanto aos bens jurídicos disponíveis.

Ademais, como aponta Crespo, verifica-se uma disseminação doutrinária, social e midiática a estabelecer uma correlação entre crimes informáticos e qualquer prática delitiva perpetrada mediante o uso de tecnologias.[200]

3.4. Principais crimes informáticos em espécie

A partir da classificação proposta, traça-se um panorama dos principais crimes informáticos alusivos a bens jurídicos individuais disponíveis, que são aqueles que guardam relação mais intrínseca à vertente positiva e protagonista do livre desenvolvimento da personalidade dos usuários no ambiente virtual.

Parte-se do crime informático próprio por excelência, o delito de invasão de dispositivo informático. Na sequência, há breve abordagem dos delitos impróprios *lato sensu*. Por fim, em razão do enfoque desta pesquisa, procede-se a uma análise dos principais crimes patrimoniais informáticos impróprios *stricto sensu* e mediatos, apresentando-se breve conclusão sobre o papel protagonista da vítima na conformação típica desses delitos.

---

[199] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, p. 73.
[200] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 63.

3.4.1. Invasão de dispositivo informático (artigo 154-A do Código Penal)

Trata-se de crime comum, de modo que qualquer pessoa poderá ser sujeito passivo. Com a nova redação da modalidade prevista no *caput,* do artigo 154-A, a vítima será o usuário do dispositivo informático e, portanto, titular dos dados.[201]

O *caput* desse dispositivo possui como único verbo nuclear *invadir,* consistente em "violar ou ingressar, clandestinamente, isto é, sem autorização de quem de direito."[202] Da presença de um único verbo, contudo, emana a crítica de ser inviável a revogação da concessão para o ingresso, porquanto não se encontra tipificada a simples permanência sem autorização, diferentemente do que ocorre no tradicional delito de violação de domicílio (artigo 150, do Código Penal).[203] Logo, o excesso de permanência de acesso ao dispositivo, como no aplicativo TeamViewer (que faculta controle momentâneo ao dispositivo por terceiros), será atípico.

O objeto material da conduta é o dispositivo informático alheio, entendido como um *hardware*. Essa amplitude terminológica é corroborada pelo fato de não ser necessária conexão com a rede de computadores (Internet), como dispõe o *caput*.

De se ressaltar que, em sua redação original, o tipo penal contava com um elemento normativo especial da antijuridicidade, consubstanciado pela expressão "mediante violação indevida de mecanismo de segurança." Ocorre que era uma expressão desnecessária e pleonomástica, visto que a conotação de violação já se depreendia do verbo nuclear do tipo.[204] Se isso não bastasse, conferia restrição excessiva à conduta delitiva, porque, ao fazer alusão a mecanismos de segurança, pressupôs a transgressão de programa informático especificamente formulado para a proteção do dispositivo.

Em face dessas críticas tecidas, a Lei n. 14.155/2021 suprimiu esse elemento normativo do tipo penal, de modo que se tornou prescindível a presença de mecanismo de segurança. Assim, a princípio tornou-se típico o acesso a *pendrives* e aparelhos celulares utilizados por terceiros, ainda que não sejam protegidos por senha. De todo modo, como se verá em ulteriores

---

[201] Alteração salutar considerando-se ser passível a prática do delito pelo próprio titular do dispositivo, como em empresas ou mesmo computadores domésticos compartilhados, porém com usuários diferentes para cada membro.
[202] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte especial*. v.2, 14. ed. São Paulo: Saraiva, 2014, p. 513.
[203] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 446.
[204] CRESPO, Marcelo Xavier de Freitas. Dos crimes de inserção de dados falsos em sistemas de informação (Art. 313-A, CP) e modificação ou alteração não autorizada de sistema de informação (Art. 313-B, CP). *In:* CRESPO, Marcelo Xavier de Freitas (coord.). *Crimes contra a administração pública: aspectos polêmicos*. São Paulo: Quartier Latin, 2010.

Capítulos,[205] eventual ausência de tais mecanismos poderá trazer implicações para a conformação típica, a depender das circunstâncias do caso concreto.

Outra alteração que conferiu maior abrangência ao tipo penal consistiu na substituição da expressão "dispositivo informático alheio" por "dispositivo informático de uso alheio". Anteriormente, era necessária apenas a autorização expressa ou tácita do titular do dispositivo para a atipicidade da conduta, ainda que os dados fossem pertencentes a outro usuário. Atualmente, com essa atualização, é imprescindível a anuência do usuário do dispositivo, de modo que a vítima não será forçosamente proprietária do dispositivo.[206]

Verificado o tipo objetivo, é necessário dolo do agente, sendo a invasão culposa de dispositivo informático – embora de rara verificação prática - atípica. Ademais, é necessário o preenchimento de ao menos um dos elementos subjetivos especiais do tipo: finalidade *a) de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo; b) instalar vulnerabilidades para obter vantagem ilícita*. Ausentes ambos os elementos, novamente, a conduta será atípica. Trata-se de uma excessiva limitação de finalidades pelo legislador, que nem sequer se preocupou em expandir esse rol, frente às diversas modalidades de invasão de dispositivos informáticos já verificáveis na atualidade. Em verdade, com constante progresso tecnológico na área informática, mostra-se absolutamente contraprudecente delimitar a finalidade da invasão aos dispositivos, dada sua constante expansão.

Por integrar o tipo penal do delito, o consentimento expresso ou tácito do titular dos dados excluirá, indubitavelmente, a tipicidade da conduta. Essa estrutura típica evidencia tratar-se de crime formal, sendo prescindível qualquer resultado naturalístico de obtenção de dados ou instalação de vulnerabilidade. Em que pese Vianna e Machado entendam consistir em crime material,[207] conforme apontam Nucci[208] e Crespo[209], com o êxito na empreitada delitiva haverá

---

[205] Cf. Capítulo 5.3. (Vitimodogmática e crimes informáticos) e Capítulo 6.5. (Propostas para a autocolocação em risco nos crimes informáticos).

[206] Muito embora frequentemente o usuário corresponda ao titular, essa identificação inexiste em computadores cedidos por empresas, ou mesmo utilizados por diversos membros de uma mesma família, por meio de perfis e senhas distintos.

[207] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 98.

[208] NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020, p. 340.

[209] CRESPO, Marcelo Xavier de Freitas. Dos crimes de inserção de dados falsos em sistemas de informação (Art. 313-A, CP) e modificação ou alteração não autorizada de sistema de informação (Art. 313-B, CP). *In:* CRESPO, Marcelo Xavier de Freitas (coord.). *Crimes contra a administração pública: aspectos polêmicos*. São Paulo: Quartier Latin, 2010.

mero exaurimento do delito. Por outro lado, como se trata de delito plurissubsistente, é perfeitamente possível a tentativa.

Em que pese o mérito do legislador em inaugurar, tardiamente, o primeiro tipo penal atinente a crime propriamente digital, pecou por restringir excessivamente a conduta delitiva, fortemente inspirado em poucos casos concretos que deram ensejo à aprovação legislativa frente a inúmeras hipóteses da prática de condutas lesivas à autodeterminação informática, como se verá a seguir. Referidas limitações foram apenas parcialmente sanadas com o advento da Lei n. 14.155/2021, que promoveu alterações pontuais, insuficientes para um tratamento sistemático sobre os crimes informáticos.

3.4.1.1. Condutas lesivas atualmente abarcadas pelo artigo 154-A, caput, com a redação dada pela Lei n. 14.155/21

Como visto, a carência de mecanismo de segurança no dispositivo informático conduzia à atipicidade de qualquer invasão ou acesso indevido. Assim, era atípico inclusive acesso não autorizado a *notebooks*, *pendrives* e cartões de memória desprovidos de senha. E mais: a subtração de mecanismos físicos de autenticação, tais como *SmartCards*, *On time password* e chaves privadas (certificado digital) também não conduzia à prática de crime informático próprio.[210]

Ademais, anteriormente era prescindível a anuência do usuário não titular do dispositivo caso seu titular autorizasse o acesso, o que conduzia a violações indevidas ao bem jurídico tutelado, como o acesso por empregadores de dados pessoais no dispositivo informático de uso pessoal dos empregados, ou mesmo acesso por outros membros da família do perfil de seus familiares no aparelho de uso comum.[211_212]

---

[210] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 108.

[211] Em razão da existência de diversos *malwares* instalados sem qualquer autorização do usuário, porém, que não superam mecanismos de segurança, havia a atipicidade, exemplificativamente, da inserção de *rootkits* (que viabilizam controle sobre o próprio sistema operacional do dispositivo), injeção de *SQL* (solicitação indevida de consultas a bancos da dados) e instalação de *backdoor* (falha no próprio sistema que permite o ingresso de terceiros).

[212] Jesus e Milagre ponderam, nessas hipóteses, ser praxe a necessidade de utilização de senha para uso do mecanismo de autenticação. Sustentam oa autores, nesse sentido, que as tentativas de descoberta da senha (*password guessing*), conduziam à prática de conduta típica, caso houvesse êxito no acesso, inclusive na redação original do artigo 154-A, do Código Penal. (JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 112). Ao nosso sentir, o acesso a dispositivo informático independentemente do uso de mecanismos físicos de autenticação, após acertada digitação de senha, não configurava anteriormente o ilícito penal. Isso porque, nessa hipótese, o mecanismo de segurança automaticamente conferiria acesso ao sistema, não havendo que se falar de sua superação.

Essas deficiências, porém, foram devidamente sanadas com a alteração promovida no tipo penal quando da edição da Lei n. 14.155/2021. Por outro lado, ainda remanesce uma série de práticas lesivas não abarcadas pela nova redação do delito de invasão de dispositivo informático. Em estrita observância à legalidade, é atípica a superação de programa de proteção contra gravação, cuja finalidade é a simples obstrução à alteração de dados, não ao acesso.

Prática corriqueira dentre os iniciantes na criminalidade informática (*wannabes*) consiste na simples invasão de dispositivos alheios com vistas a obter técnicas e experiências necessárias para condutas mais sofisticadas. A finalidade do agente, portanto, se limita à superação do mecanismo de segurança, de modo que não resta preenchido elemento subjetivo especial do tipo. Apesar de não se verificar, *in abstrato*, uma conduta ofensiva à autodeterminação informática, uma invasão de dispositivo pode culminar, indiretamente, com maior vulnerabilidade oriunda de maior suscetibilidade a ataques do mecanismo de segurança, de modo a tornar seu titular vulnerável a outros acessos indevidos aptos a violar o bem jurídico tutelado.[213]

Do mesmo modo, o segundo elemento subjetivo especial do tipo mostrou-se demasiado restritivo. Não basta uma invasão do dispositivo com vistas a instalar vulnerabilidades, visto que é necessário o fim de obtenção de vantagem ilícita. Logo, a simples instalação de vulnerabilidades, sem essa ulterior finalidade, também configura conduta atípica. Ocorre que a maior suscetibilidade do dispositivo informático ao acesso indevido por terceiros, por si, gera uma lesão à autodeterminação informática.[214]

Ademais, como não há previsão legal acerca da finalidade de inserir dados, a simples invasão com esse intuito não perfaz crime do artigo 154-A, ainda que destinado à obtenção de vantagem ilícita, como na hipótese de inserção de informações em banco de dados de pessoas que recebem auxílio governamental.[215]

Mesmo com as alterações legislativas, deve-se pontuar que, caso a invasão não viole o dispositivo informático em si, mas somente seus aplicativos, a conduta remanesce atípica. Com isso, o simples acesso indevido ao aplicativo Whatsapp ou Telegram não perfaz o tipo objetivo do delito previsto no artigo 154-A do Código Penal.[216]

---

[213] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 71.

[214] Se não bastasse, para além da indeterminação da expressão, Sydow faz menção ao fato de se encontrar no plural, de maneira que a intenção de instalar uma única vulnerabilidade – ironicamente – culminaria com a atipicidade da conduta, em observância ao princípio da legalidade. (SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 448).

[215] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016, p. 109.

[216] COSTA, Adriano Sousa; FONTES, Eduardo; HOFFMANN, Henrique. Lei 14.155/21 incrementa punição de crimes eletrônicos e informáticos. *Consultor Jurídico*, mai. 2021.

Em verdade, vê-se que o simples acesso indevido ao dispositivo informático deveria perfazer as elementares do tipo objetivo, consistindo a efetiva obtenção/adulteração/destruição de dados ou de vantagem ilícita – aliada aos elementos subjetivos a ela atrelados - em mero exaurimento do crime.

Aliás, o próprio verbo nuclear do tipo merece ressalvas, porquanto com o termo "invadir" depreende-se, em geral ato violento ou hostil[217] quando, em verdade, deve-se apenar qualquer acesso desprovido de autorização tácita ou expressa do usuário, o que pode ser sintetizado nos termos "acessar indevidamente".[218] Dessa forma, seria possível abarcar três das principais modalidades de acesso não autorizado: a) simples invasão do dispositivo sem finalidade ulterior; b) acesso a quaisquer dados armazenados; c) alteração e sabotagem de dados.[219]

3.4.1.2. Figura equiparada a invasão de dispositivo informático

O §1º do artigo 154-A estabelece uma figura equiparada, consistente na produção, oferta, distribuição, venda ou difusão de dispositivo ou programa de computador com o intuito da prática da conduta descrita no *caput*. Como pontua Bitencourt, trata-se de delito vinculado à conduta originária de invasão de dispositivo informático, de modo que sua finalidade (ou seja, o elemento subjetivo especial do injusto) deverá estar direcionada a todos os elementos deste crime.[220] Assim, busca-se incriminar a produção e demais condutas de divulgação de códigos maliciosos como *Keyloggers*, *Trojans*, *Worms* e *Distributed Denial of Service*.

Não obstante a intenção do legislador de coibir a prática do delito previsto no *caput,* do artigo 154-A, do Código Penal, verifica-se que a criminalização da simples produção de dispositivo ou programa de computador apto a invadir dispositivo informático consiste em uma antecipação da tutela penal em momento prévio ao risco concreto ao bem jurídico autodeterminação informática. Verifica-se, destarte, um incremento punitivo de ato

---

[217] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 444.

[218] Sydow defende o termo "intrusão", enquanto faz menção ao "acesso não autorizado". A fim de reforçar o papel do usuário em anuir com o acesso, bem como reconhecendo a possibilidade de sua manifestação tácita (inclusive em casos de urgência, como a proteção do dispositivo alvo de ataques), entende-se pela melhor adequação da expressão "acesso indevido". (SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021).

[219] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 65.

[220] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte especial*. v.2, 14. ed. São Paulo: Saraiva, 2014, p. 518.

preparatório, uma faceta perniciosa da sociedade de risco há muito criticada por Silva Sánchez, revelada como uma das causas (ilegítimas) da expansão do direito penal.

E mais: equiparou-se indistintamente esse agente àquele que efetivamente invade dispositivo informático de uso alheio (ou seja, quem efetivamente expõe a risco concreto o bem jurídico), violando-se o princípio da culpabilidade.[221]

A tipificação de atos preparatórios é possível sempre que legalmente prevista como delito autônomo. Ao nosso sentir, porém, deve ser limitada a hipóteses muito exíguas, em que haja risco concreto ao bem jurídico tutelado, o que não se vislumbra no §1º, do artigo 154-A, por se tratar de conduta muito afastada do momento de execução dentro do *iter criminis* da conduta descrita no *caput*. Neste caso, com isso, verifica-se violação ao princípio da ofensividade, subsidiariedade e fragmentariedade do direito penal.

3.4.1.3. Ação Penal

Conforme dispõe o artigo 154-B, via de regra, a ação será pública condicionada à representação, o que se mostra condizente com a natureza disponível do bem jurídico tutelado. É um alinhamento adequado, inclusive, com a atipicidade da conduta na hipótese de anuência da vítima com a disposição dos dados ou acesso ao dispositivo. Assim, o relevante papel desempenhado pela vítima reverbera sobre a natureza da ação penal.

Por outro lado, diante da prática delitiva em face da administração pública direta ou indireta de quaisquer dos poderes dos entes da federação ou contra empresa concessionária de serviço público, a ação penal será pública incondicionada. Nessas hipóteses, o bem jurídico deixa de ser disponível, por dizer respeito ao interesse público. Aliás, não se trata de crime digital próprio, mas sim misto, porquanto se tutela simultaneamente o bem jurídico a administração pública. Por essa razão, foi acertada a definição da natureza da ação penal.[222]

---

[221] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 457. Ora, caso deflagrado o início da execução, verificado o liame subjetivo entre o agente detentor do dispositivo ou programa de computador e aquele que promoverá a invasão do dispositivo informático, não há qualquer óbice para a incidência de modalidade tradicional de concurso de agentes, nos ditames do artigo 29, do Código Penal.

[222] Contudo, há uma patente impropriedade ao se fixar representação do ofendido na hipótese do artigo 154-A, §1º, tendo em vista que a simples produção, oferta, distribuição, venda ou difusão de código malicioso não possui vítima determinada, por se tratar, como visto, de crime de perigo abstrato, em razão de sua nítida antecipação à conduta lesiva. Logo, a única hipótese factível consistiria em se localizar a vítima da conduta descrita no *caput*, o que se torna espécie de condição objetiva de punibilidade daquele delito. (NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020, p. 344).

3.4.1.4. Vítima no crime de invasão de dispositivo informático

A redação do dispositivo reforça o papel protagonista do usuário, visto que sua autorização tácita ou expressa para acesso ao dispositivo implicará abstenção da tutela penal. Conforme Vianna e Machado, "a autorização tácita é aquela fornecida por atos que demonstrem inequivocamente a permissão do titular dos dados para que o agente os acesse. Como exemplo, pode-se citar o fornecimento de login de usuários e senha para um amigo."[223]

No entanto, há outras hipóteses mais complexas. Emergem dificuldades quanto à capitulação da corriqueira prática de *phishing*, mediante engenharia social, na qual o agente, por meio de artifício ou ardil, induz a vítima a fornecer informações pessoais (por exemplo, informações de acesso a um programa ou aplicativo). Assiste razão a Brito, ao sustentar que não há preenchimento do tipo objetivo por inexistir invasão do dispositivo. É possível a prática de *phishing* em que a vítima, na crença de utilizar ou instalar algum arquivo funcional – ou seja, não ciente de sua real finalidade –, voluntariamente desabilita o mecanismo de segurança de seu dispositivo informático e autoriza acesso livre ao agente. Para Brito, neste último caso haverá o crime porque a autorização de acesso mediante engano configuraria uma violação ao dispositivo.[224]

Quanto a este ponto, no entanto, merece prestígio o raciocínio de Jesus e Milagre acerca do instituto do acordo em direito penal. Comparando-se com o delito de violação de domicílio, se uma pessoa autoriza a entrada a seu lar, ainda que mediante engano, não está preenchido o tipo penal.[225] Isso porque o erro quanto aos motivos do assentimento apenas é relevante, para fins penais, quando não seja elementar do próprio delito, o que configuraria consentimento do ofendido – hipótese majoritariamente rotulada como causa supralegal excludente da antijuridicidade. Por conseguinte, sempre que integre a estrutura típica do delito, como também ocorre no crime informático próprio ora tratado, de qualquer modo se estará diante de conduta atípica.

Por outro lado, caso o agente iluda a vítima, mediante algum artifício, a involuntariamente autorizar acesso ao dispositivo informático (*phishing scam* mediante *malware* ou código malicioso) após receber e autorizar um arquivo ou código fornecido, restará preenchido o tipo objetivo, desde que presente o elemento especial subjetivo.

---

[223] VIANNA, Túlio; MACHADO, Felipe. Crimes Informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 96.
[224] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 70.
[225] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016, p. 106.

Resta ainda a prática de *phishing* mediante *keylogger*, *screenlogger* ou outros programas de captura de dados, em que a vítima apenas executa – voluntariamente porém inciente da real finalidade – um arquivo que remete dados e teclas digitadas ao atacante, todavia, não lhe faculta qualquer acesso ao dispositivo. Ausente invasão, não se está diante do tipo penal previsto no artigo 154-A. podendo configurar, a depender do caso concreto, interceptação telemática (artigo 10, da Lei n. 9.296/96) ou furto qualificado).[226]

Verifica-se, assim, que se impõe redobrada atenção à conduta da vítima no momento de autorizar voluntariamente acesso por terceiros a seu dispositivo, posto que essa hipótese de acordo excluirá a conduta típica nos termos do artigo 154-A do Código Penal. A título exemplificativo, cite-se a corriqueira conduta de autorizar um programa da Internet a efetuar alterações no disco rígido do computador, não configurando crime informático próprio.

Sob a ótica da vítima, verifica-se que a Lei n. 12.737/2012 conferiu papel protagonista ao titular do bem jurídico tutelado. Embora de modo involuntário – porquanto várias hipóteses de atipicidade derivavam, em verdade, de atecnia e da usual maneira de legislar com base em casos concretos midiatizados-, o legislador atribuía à vítima o ônus de se atentar e proteger contra algumas condutas no meio ambiente digital. Em síntese: a) deveria ser instalado mecanismo de segurança no dispositivo; b) esse mecanismo deveria estar ativado; c) não poderia haver autorização tácita de acesso, inclusive perpetrada mediante artifício, ardil, engodo; d) bastava a autorização do titular do dispositivo, de modo que o titular dos dados, caso diverso, não receberá tutela penal (poderá buscar reparação pela LGPD, porém); e) *password guessing* era conduta atípica, o que impõe responsabilidade na escolha de senhas mais complexas, minimizando as chances de êxito dos agentes.

Com a edição da Lei n. 14.155/2021, os problemas pontuados nos itens “a”, “b” e “d” foram sanados. De qualquer modo, apesar de se tornar desnecessária a presença de mecanismo de segurança ativo para sua invasão, trata-se de cautela mínima e usual a ser adotada pelos usuários. Com isso, deve-se avaliar, no caso concreto, a razão pela qual esse mecanismo não estava ativado: se se tratar de omissão absolutamente desidiosa e consciente da vítima, sendo certo que a ativação do mecanismo obstaria a prática delitiva, deve-se perquirir sobre eventuais efeitos para a responsabilização penal do autor. Essa, aliás, era a *ratio* do legislador quando da redação originária do artigo 154-A, do Código Penal: se o usuário não se esforçasse

[226] Em analogia com o delito de invasão de domicílio, essa prática é equiparável ao morador que traz objetos a sua residência que contenham câmeras escondidas. Essas câmeras, por sua vez, remetem informações do local ao agente, sem que este possua qualquer acesso direto a seu interior. (JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Op. cit.*, p. 146).

minimamente para proteger seu dispositivo, não seria necessária a tutela penal. Ocorre que, como visto, tal limitação generalizante ínsita ao próprio tipo penal culminava com injustiças, posto que outrem poderia desativar o mecanismo de segurança, ou mesmo poderia se tratar de usuário vulnerável merecedor de tutela penal.

Por outro lado, a redação atual do dispositivo ainda confere excessiva limitação a algumas hipóteses, penalizando a vítima por condutas não situadas em sua esfera de risco. A título exemplificativo: a) com a simples invasão do dispositivo por um *wannabe* – logo, com a pura finalidade de superar mecanismo de segurança ou instalar vulnerabilidades– e ulterior acesso de dados por terceiro, sem liame subjetivo prévio anterior entre si, a conduta será atípica para ambos; b) se a vítima voluntariamente faculta o acesso a seu dispositivo, induzida mediante prática de *phishing*, não haverá prática do delito do artigo 154-A. Isso, contudo, não necessariamente configura conduta culposa de sua parte, notadamente em se tratando de indivíduos vulneráveis.

Assim, apesar das alterações promovidas, o legislador ainda peca pela baixa qualidade técnica da redação do tipo penal, sem efetuar o adequado sopesamento no tocante às diversas – e crescentes – condutas aptas a lesar o bem jurídico tutelado. Em verdade, a complexidade do ambiente informático impõe necessária análise casuística e compreensão do usuário concreto para se perquirir acerca da lesão ao bem jurídico tutelado, o que não pode ser exercido aprioristicamente pelo tipo penal abstrato, quer a favor, quer contra a configuração de conduta penalmente típica.

Em suma, apesar da excessiva restrição e da involuntariedade do legislador com relação ao resultado obtido, a redação do artigo 154-A, do Código Penal, converge no sentido da era da informação e da sociedade de risco, reconhecendo a importância do papel da vítima no meio ambiente virtual. Disso decorre a relevância da vitimodogmática e do funcionalismo penal na seara dos crimes informáticos, quer para delimitar a esfera de responsabilidade da vítima – nem sempre responsável pela autorização de acesso a seu dispositivo -, quer para viabilizar a criação de tipos penais adequados à tutela do bem jurídico afetado.

3.4.2. Crimes informáticos impróprios *lato sensu*

Como visto, em sentido amplo, a prática de crimes informáticos impróprios diz respeito à violação de bem jurídico diverso da autodeterminação informática, em razão de finalidades ulteriores do agente. Caso inexista qualquer violação a esse bem jurídico, tornando-se o meio virtual mero instrumento da conduta, está-se diante de crimes informáticos impróprios *stricto*

sensu. Há ilimitados delitos enquadráveis nesta categoria, considerando-se o surgimento de novos mecanismos de prática virtual de delitos tradicionais.

Tem sido frequente a prática de crimes contra a honra por meios virtuais, notadamente em redes sociais como Facebook, Twitter, Instagram, em que os agentes praticam calúnia, injúria ou difamação em desfavor de seus algozes. Também é recorrente a prática de racismo. Ademais, muitos usuários, valendo-se do anonimato ou da dificuldade de sua localização, proferem ameaças, bem como praticam apologia e incitação a crimes nesse ambiente.

Não se pode olvidar o delito de violação de direitos autorais, com simples *download* de conteúdo sem autorização de seu titular. Multiplicam-se ainda casos de participação em suicídio (como o caso do aplicativo Baleia Azul), pornografia infantil e, inclusive, crimes contra o Estado Democrático de Direito (antes violadores da revogada Lei de Segurança Nacional). Tornam-se, com isso, infindáveis as possibilidades de práticas de delitos informáticos *stricto sensu* na atualidade.

A seu turno, caso haja concomitantemente violação ao bem jurídico autodeterminação informática, está a se falar de crime informático misto ou mediato, conforme se perfaça um único tipo penal (hipótese em que será misto) ou incida o princípio da consunção em função do concurso aparente de crimes (absorvendo-se o delito informático próprio, em que haverá crime informático mediato). Recentemente, o delito de furto qualificado mediante fraude por meio informático recebeu tipificação própria, de modo que deixou de ser crime informático mediato, tornando-se misto.

Por fim, assim como nos delitos informáticos impróprios *stricto sensu*, há uma incontável gama de delitos mediatos, porquanto incidente a norma geral do princípio da consunção. Logo, sempre que, para a prática de delito-fim, haja a prática do delito-meio de violação de dispositivo informático, está-se diante de delito informático mediato. A título exemplificativo, a invasão de dispositivo informático com intuito de praticar extorsão, como nos casos de *ramsomware*, como aquela em face do Superior Tribunal de Justiça. Pode-se cogitar, inclusive, da prática de homicídio, com a invasão de equipamentos eletronicamente controlados, como jatos e caças não tripulados, veículos automatizados, entre outros.

3.4.3. Crimes informáticos patrimoniais impróprios e mediatos

Não se pode olvidar que parcela significativa dos delitos praticados no ambiente virtual é praticada com o escopo de obtenção de vantagem econômica, destacando-se os delitos patrimoniais. Essas condutas vêm marcadas por mecanismos ardilosos como *phishing* e

engenharia social, sendo essencial uma análise mais detida. Destacam-se, assim, os delitos de dano (crime informático mediato, nos moldes da legislação atual), furto qualificado mediante fraude por dispositivo informático ou eletrônico (crime informático misto), fraude eletrônica e estelionato (ambos crimes informáticos impróprios *stricto sensu*).

Os crimes patrimoniais de furto, dano e apropriação indébita apresentam como objeto material de seus respectivos tipos penais a elementar "coisa". De início, impende avaliar se os dados pessoais armazenados virtualmente são enquadráveis sob essa concepção.

Segundo Bitencourt, coisa é "tudo que se possa constituir objeto da ação física de subtrair, isto é, *coisa corpórea* passível de ser deslocada, apreendida ou transportada de um lugar para outro."[227] Acrescenta o autor que elementos intangíveis, caso passíveis de apreensão ou consumo, também são enquadráveis no conceito.

Aprofundando-se na seara informática, Vianna[228] defende que "dados" se amoldam ao conceito de coisa, sendo despicienda sua materialidade a partir de interpretação analógica da elementar típica. Assim, para o autor, o legislador "disse menos do que almejava dizer" ao formular o conceito de "coisa".

Discorda-se dessa posição. Historicamente, os crimes patrimoniais foram delineados pelo legislador sempre lastreados em bens tangíveis, materiais, inclusive porque, à época da elaboração do Código Penal, pouco se cogitava acerca de informática, que se encontrava em estágio inicial, limitada a setores de inteligência governamentais.[229_230] Como aponta Guardia, dados são meros impulsos eletromagnéticos não perceptíveis, tendo em vista que o usuário apenas vislumbra o processamento eletrônico.[231] Por essa razão, não são subsumíveis ao conceito clássico de "coisa".[232]

---

[227] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte especial*. v. 3, 14. ed. São Paulo: Saraiva, 2014, p. 36.

[228] VIANNA, Túlio Lima. Do delito de dano e sua aplicação ao direito penal informático. *Revista de derecho informático*, n. 62, set. 2003 *apud* CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 72.

[229] Aliás, tanto a intangibilidade não foi contemplada pelo legislador que a energia elétrica foi equiparada a coisa pelo artigo 155, §3º, do Código Penal. Trata-se de um reconhecimento de que subtração de energia, os denominados "gatos", não estavam abarcados pelo *caput* do dispositivo.

[230] Se não bastasse, como aponta Crespo, foram elaboradas leis específicas com vistas à proteção de propriedade intelectual e propriedade industrial, o que reforça a inviabilidade de informações serem abarcadas pelos crimes patrimoniais por excelência. (CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 73).

[231] GUARDIA, Diego L. Los delitos informáticos frente al concepto tradicional de "cosa". *Ciencias Penales Contemporáneas: Revista de Derecho Penal, Procesal Penal y Criminología*, Mendoza, v. 2, n. 4, p. 145-181, 2002, p. 156.

[232] Dessa forma, em respeito ao princípio da legalidade, o conceito de "coisa" deve ser limitado a elementos tangíveis. Uma interpretação em sentido diverso culminaria com inadequada utilização de analogia *in malam partem*, posto que seria verdadeira integração de lacuna normativa.

Dessa forma, em sede de delitos informáticos, apenas *hardwares*, ou seja, suportes físicos como computadores, CDs, *pendrives*, *HD*s são passíveis de subtração, danificação ou apropriação para fins de crimes patrimoniais. O acesso, cópia, destruição ou subtração tão somente de dados informáticos, caso não configurem o delito previsto no artigo 154-A, do Código Penal, serão condutas atípicas.

Por essa razão, Crespo propõe a criação de um tipo penal apto a abranger a alteração, destruição e supressão de dados eletrônicos, prescindindo-se de prévia prática do delito de invasão de dispositivo informático.[233] Nesse sentido, o denominado dano informático seria apto a preencher o vazio legislativo ao incluir dados como objeto material da conduta.[234]

Do mesmo modo, não há tipificação do delito de furto com a mera subtração de dados eletrônicos. Por outro lado, é prática muito frequente a obtenção de informações pessoais e senhas com diversas finaliades. Primeiramente, essa subtração pode ocorrer mediante *phishing scam*, em que a vítima consente – mediante engano, ardil – com o acesso do programa malicioso a seu dispositivo. Também é possível que sejam instalados, ainda que sem o consentimento da vítima, programas como *keyloggers*, aptos a captar a senha digitada. Essas modalidades, como visto, não configuram a prática do artigo 154-A, do Código Penal.

Com isso, verifica-se que a Lei n. 14.155/2021 promoveu alterações demasiado tímidas no tocante à criminalização de condutas lesivas no ambiente informático, deixando de criminalizar tanto a subtração como a destruição de dados eletrônicos como delitos independentes da invasão de dispositivo informático. Assim, caso não haja um crime-fim ulterior, como a prática de estelionato ou furto mediante fraude, essas condutas serão atípicas.[235]

Quanto aos crimes informáticos mistos, de particular relevância é o furto qualificado mediante fraude por meio de dispositivo informático. Por meios informáticos são empregados artifícios para reduzir a vigilância da vítima, permitindo-se a obtenção de dados necessários para a subtração de valores, notadamente senhas para transferências em instituições financeiras.

O dinheiro, objeto material nessa hipótese, apesar de intangível, não perde sua característica material, o que permite o enquadramento como "coisa" para fins do artigo 155, *caput* e parágrafos, do Código Penal. Isso porque, para além da indissociabilidade entre o numerário eletronicamente constante da conta bancária de seu titular e as cédulas monetárias a

---

[233] CRESPO, Marcelo Xavier de Freitas. *Op. cit.*, pp. 73-74.
[234] AROCENA, Gustavo Alberto. Acerca del principio de legalidad penal y de hackers, crackers, defraudadores informáticos y otras rarezas. *Ley, Razón y Justicia*, v.4, n. 6, 2002, p. 20-21.
[235] Cite-se, a título exemplificativo, a subtração de dados pessoais para posterior revenda a empresas de publicidade virtual, que irão direcionar propagandas e e-mails ao usuário, conduta penalmente atípica.

ele correspondentes, verifica-se sua efetiva apreensão, posto que não pode ser simplesmente copiado (*ctrl + C).*

Se isso não bastasse, não se pode olvidar que o bem jurídico patrimônio é indissociavelmente relacionado à sua vertente econômica, ou seja, monetária. Dessa forma, predomina que o mero valor sentimental do bem, ou simples relação de propriedade não são aptos a configurar lesão (conceito jurídico de patrimônio). Assim, qualquer subsunção do termo "coisa", sob o conceito econômico de patrimônio, necessariamente será monetariamente mensurável, de modo que seria um contrassenso excluir de sua interpretação valores em espécie, ainda que intangíveis.[236]

Referida discussão restou sobremaneira pacificada com a edição do artigo 155, §4º-B, do Código Penal, em que se previu a prática de furto mediante fraude por meio de dispositivo eletrônico ou informático, ou ainda, por outro meio fraudulento análogo, consagrando-se sob o aspecto legislativo a possibilidade de subtração de valores por meios informáticos. Característica marcante dessa prática consiste em afastar a vigilância da vítima, mediante artifícios promovidos por intermédio de dispositivos informáticos ou eletrônicos. Antes da Lei n. 14.155/2021, porém, referida prática se enquadrava como furto qualificado mediante fraude.

Segundo o artigo 155, §4º-B, do Código Penal, impõe-se pena de reclusão de quatro a oito anos para a prática de furto mediante fraude por meio de dispositivo informático ou eletrônico. O tipo objetivo é configurado independentemente: a) da violação de mecanismo de segurança; b) de conexão à Internet; c) de utilização de programas maliciosos, como *malwares*, ou meios fraudulentos análogos, como *spywares*. Essa tipificação mostra-se adequada para abarcar as diversas modalidades de execução do delito. Assim, podem ser abrangidas práticas de engenharia social, casos em que a subtração de valores pode ocorrer por meio de *malwares* que não violem mecanismos de segurança, como o *keyloggе*r. Do mesmo modo, a invasão de aplicativos em *smartphones* para fins de subtração de valores perfaz a conduta típica.[237]

---

[236] Há de se reconhecer, nesse contexto, que a prática de furto por meio de *Internet Banking* configura a prática de crime informático mediato – visto que pressupõe acesso indevido a dados do titular dos valores com vistas a fim patrimonial.

[237] Nota-se que restou abrangida também a prática de furto mediante fraude precedida de invasão de dispositivo informático. Antes do advento da Lei n. 14.155/21, a prática de furto mediante fraude absorvia o delito previsto no artigo 154-A do Código Penal, por força do princípio da consunção. Ocorre que, por força do novo delito de furto mediante fraude por meio de dispositivo eletrônico, ainda que o agente nem sequer logre êxito em invadir o dispositivo da vítima, caso presente a intenção de subtração de bens ou valores, sempre se estará diante da modalidade do artigo 155, §4º-B, do Código Penal (na hipótese, por tentativa), por incidência do princípio da especialidade.

Depreende-se consistir em delito informático misto, posto que, para a subtração de valores (prática de furto), o agente viola o bem jurídico autodeterminação informática, que encontra previsão no bojo do tipo penal.

Deve-se destacar ainda que há previsão de causa de aumento em se tratando de vítima idosa ou vulnerável. Por idoso deve-se compreender o indivíduo com idade superior a 60 anos, nos termos do artigo 1º, da Lei n. 10.471/2003. E, na carência de explicitação do termo vulnerável, deve-se empregar aquela conceituação prevista no artigo 217-A, *caput* e §1º, do Código Penal, alusiva ao delito de estupro de vulnerável. Destarte, terão essas características pessoas com idade inferior a 14 anos, além de indivíduos que, em razão de enfermidade ou deficiência mental, não possuam o discernimento para a prática de certos atos. Deve-se destacar, na hipótese, ser imprescindível que o agente (*cracker* ou não) tenha ciência de que se trata de pessoa vulnerável para a incidência da respectiva causa de aumento.

A Lei n. 14.155/2021, ao traçar indivíduos particularmente vulneráveis por meio da implementação de causas de aumento dessa nova modalidade de furto qualificado, é apta a traçar referenciais para apuração de quais vítimas merecem especial tutela na seara de crimes informáticos. Fornece, assim, indicativos não exaustivos acerca para a vitimodogmática, sob uma ótica abstrata e genralizante de grupos de pessoas. Resta, ainda, perquirir acerca de elementos que possam representar vulnerabilidade em casos concretos, bem como o reverso da moeda: quais fatores relativos às vítimas que, caso presentes, devam atenuar ou, até mesmo, excluir a responsabilidade do agente.

Por fim, é extremamente comum a obtenção de dados diretamente da vítima, mediante engenharia social, por meio de envio de e-mails, cartas ou ligações fraudulentas. Afinal, ainda hoje o mecanismo mais simples e eficiente de obtenção de informações consiste em perguntá-las à vítima.

Em poder dos dados necessários, então, o agente acessa fraudulentamente a conta bancária e subtrai os valores do correntista. Observe-se que, conforme consolidado na jurisprudência, tratava-se da prática de furto mediante fraude, considerando-se que o titular (vítima) não entrega voluntariamente qualquer quantia ao agente. Atualmente, com a edição da Lei n. 14.155/2021, criou-se o tipo penal denominado fraude eletrônica (artigo 171, §2º-A, do Código Penal), de modo que a prática deixou de ser tipificada como furto.

Diferentemente da prática prevista no artigo 155, §4º-B, não há invasão de dispositivo informático ou emprego de meios fraudulentos para propiciar uma subtração sub-reptícia de dados pessoais e, com isso, de valores do usuário. Nessa hipótese, a vítima fornece seus dados

conscientemente – como número do cartão e senha –, sem saber que se trata de um esquema fraudulento.

O aspecto diferencial consiste no emprego de meios informáticos ou eletrônicos para a obtenção das informações, por meio de: a) redes sociais, sendo muito comuns anúncios fraudulentos de venda de produtos e serviços, como no Facebook e Instagram; b) contatos telefônicos, em que indivíduos solicitam a confirmação de dados bancários ou o empréstimo de valores; c) e-mail, passando-se por organizações famosas, empresas, instituições financeiras ou órgãos públicos para a cobrança de valores, além de requisição de empréstimos, recebimento de herança, entre outros; d) outros meios fraudulentos análogos, como falsos *websites*, notadamente de leilões, venda de automóveis e outros.

Para o delito de fraude eletrônica previu-se uma única causa de aumento, consistente na prática do delito por meio de servidor situado fora do território nacional. Deixou-se de reconhecer, na linha do artigo 155, §4º-B, a presença de grupos especialmente vulneráveis, o que revela um tratamento assistemático por parte do legislador. Afinal, impunha-se uniformidade de abordagem para os delitos, considerando-se que em ambos pode haver exploração da vulnerabilidade informática de suas vítimas.

Deve-se ponderar que na hipótese de fraude eletrônica não se vislumbra violação ao bem jurídico autodeterminação informática, de modo que se trata de crime informático impróprio *stricto sensu*. Em verdade, o meio digital se tornou apenas nova ferramenta para sua prática, maximizando o alcance do ardil. Afinal, mediante engenharia social, basta envio de e-mails fraudulentos, criação de websites falsos, aptos a atrair a confiança de elevado número de pessoas.

3.5. Ponderações sobre os crimes informáticos atualmente vigentes

A prática de crimes informáticos próprios, impróprios e mediatos não é mais alheia ao legislador penal. Teve sua inauguração expressa com a Lei n. 12.737/2012, porém ainda de forma limitada. Aliás, como sói, no Brasil adotou-se o caminho inverso, inaugurando-se a tutela informática por meio de legislação criminal, sobrevindo regulamentação cível tão somente com o Marco Civil da Internet e a LGPD, em 2014 e 2018, repectivamente.

O primeiro delito informático próprio recebeu, como visto, tipificação atécnica e excessivamente limitada, quer pelos elementos objetivos, quer subjetivos do tipo penal. A reforma promovida pela Lei n. 14.155/2021 sanou algumas questões relevantes, porém remanescem atípicas diversas condutas potencialmente lesivas, exemplificando-se: a) a invasão

do dispositivo por *wannabes*, sem ulterior finalidade de obtenção de dados ou instalação de vulnerabilidades; b) a invasão de aplicativos e redes sociais, porém não do dispositivo informático em si; c) a anuência da vítima com o *download* de *malware*, quando submetida a engano.

Inclusive em função da pandemia de COVID-19, que impulsionou a utilização da Internet e, com isso, de delitos nela praticados, ganharam força novos projetos legislativos referentes aos delitos informáticos. A Lei n. 14.155/2021 incluiu dois novos crimes que tipificam as fraudes mais comuns perpetradas por meio de dispositivos informáticos, com a necessária abrangência para conter as diversas modalidades desses delitos patrimoniais.

Ocorre que, como de costume, apresentaram-se alterações legislativas pontuais marcadas por maior rigor nas sanções, sem, contudo, uma preocupação sistemática ou com viés político-criminal – tanto para efetiva prevenção desses delitos, como mensuração das consequências das novas tipificações. Nesse esteio, os delitos de furto mediante fraude por meio de dispositivo informático e fraude eletrônica apresentam, excluídas eventuais causas de aumento, pena de reclusão de quatro a oito anos. Parte-se, com isso, de pena-base equiparável ao delito de roubo, ou mesmo de furto qualificado mediante emprego de explosivo, cujos potenciais lesivos são evidentemente maiores. Emerge, com isso, notória violação aos princípios da intervenção mínima – impondo-se penas superiores àquelas estritamente necessárias para se coibir o delito - e culpabilidade – posto que o grau de censurabilidade da conduta é inferior à pena efetivamente cominada.

Se não bastasse, careceu o legislador de lógica ao menos em dois pontos fulcrais: a) ao excluir da modalidade qualificada a prática de estelionato por dispositivos informáticos em que a vítima diretamente transfere valores ao agente; b) ao não estender as causas de aumento atinentes à vulnerabilidade das vítimas, previstas no artigo 155, §2º-B, ao delito de fraude eletrônica.

Por outro lado, verifica-se uma preocupação pioneira com a vulnerabilidade das vítimas na seara informática, marcada pelas respectivas causas de aumento previstas no novo delito de furto qualificado, o que apenas inaugura o debate legislativo sobre o tema. A preocupação do legislador em tutelar indivíduos particularmente vulneráveis no ambiente informático mostra-se consentânea com a tutela constitucional do direito fundamental à autodeterminação informativa, em que se busca assegurar uma tomada de decisão livre por seus titulares, de modo a proteger titulares de dados pessoais mais aptos a ter sua liberdade violada no ambiente virtual.

Acaba-se de inaugurar legislativa e doutrinariamente o estudo do usuário na esfera penal perante bens jurídicos disponíveis por excelência. Ainda há carência de abordagem, sob a ótica

penal, do papel protagonista desempenhado pelo usuário médio. Essa ótica é necessária ao se fundamentar a própria tutela desses bens jurídicos no livre desenvolvimento da personalidade, de modo que uma eventual renúncia ou exposição a risco, na sociedade atual, consistirá em verdadeira manifestação da personalidade e, com isso, exercício do bem jurídico. É essencial, com isso, o reconhecimento do protagonismo dos usuários no ambiente virtual pelas ciências criminais, com particular destaque à autodeterminação informática e ao patrimônio. Apenas com essa análise haverá integral e devida observância aos princípios penais da intervenção mínima e da culpabilidade.

Nesse contexto, impõe-se um aprofundamento do papel da vítima na seara dos delitos informáticos, para se perquirir acerca de: a) elementos abstratos de vulnerabilidade; b) elementos concretos de vulnerabilidade; c) elementos concretos em que incide a autorresponsabilidade ou sua autocolocação em risco, aptas a abrandar ou excluir a responsabilidade do agente – ainda que não se trate de consentimento ou acordo do titular. Este último aspecto ganha particular relevância em razão do rigor com que apenados os delitos informáticos, mormente aqueles de viés patrimonial, o que poderia culminar com penas desproporcionais a depender do caso concreto. Destarte, busca-se uma visão sistemática e abrangente desses delitos, com a correspondente cautela para a subsunção ao tipo penal, conferindo-se necessária consideração a aspectos político-criminais.

4. ABORDAGEM CRIMINOLÓGICA E VITIMOLÓGICA DOS CRIMES INFORMÁTICOS

A construção dos crimes informáticos objeto da presente pesquisa (alusivos à autodeterminação informática e ao patrimônio) apresenta um denominador comum: o fundamento constitucional no livre desenvolvimento do indivíduo, característica que cerca os bens jurídicos individuais disponíveis como manifestação precípua da dignidade da pessoa humana.

Como visto no Capítulo anterior, a tutela penal legislativa conferida pelo ordenamento pátrio na tutela dos crimes informáticos em espécie perpassa – voluntária ou involuntariamente – pela noção de autorresponsabilidade do usuário, como protagonista do ambiente informático em prol do livre desenvolvimento de sua personalidade, conferindo especial enfoque sobre sua atuação para a conformação da responsabilidade penal. Contudo, o legislador tem demonstrado exacerbada atecnia na elaboração dos tipos penais.

Neste Capítulo, buscam-se fundamentos empíricos para o desenvolvimento dos preceitos constitucionais liberais relacionados aos delitos informáticos e ao papel central que recai sobre os usuários no ambiente virtual. Afinal, a Constituição em um Estado Democrático de Direito enseja constantes aportes da realidade para sua conformação, refletindo valores da sociedade vigente.

Nesse contexto, na seara penal emerge a relevância da compreensão criminológica dos delitos informáticos. E a vitimologia é de particular relevância para a compreensão dos usuários virtuais não como meros sujeitos passivos do delito, mas como uma figura central que pode contribuir para o delito. Os estudos vitimológicos emergem em um fenômeno de resgate do papel desempenhado pela vítima, após as atrocidades praticadas durante a Segunda Guerra Mundial, reconhecendo-a como ser dotado de dignidade e que, portanto, deve ser considerado no bojo do fenômeno delitivo. Assim, a vitimologia dialoga diretamente com os valores constitucionais da liberdade e da dignidade humana, pois enxerga a pessoa da vítima como ser racional e digno de direitos.

Para tanto, neste Capítulo analisam-se as teorias criminológicas tradicionais, além das promissoras propostas emergentes na seara informática. Com base nas principais teorias criminológicas informáticas, quais sejam, a teoria das atividades rotineiras e a prevenção situacional do crime, visa-se a traçar os principais comportamentos a ser adotadas pelas vítimas como medidas preventivas de delitos praticados virtualmente. Trata-se do reflexo do livre

desenvolvimento da personalidade no ambiente virtual, emergindo a autorresponsabilidade como aspecto inerente à sociedade de risco informática.

Com isso, em permanente diálogo com a criminologia, a garantia constitucional do livre desenvolvimento da personalidade aponta que, nos crimes informáticos ora analisados, o comportamento arriscado da vítima poderá trazer repercussões penalmente relevantes na consumação delitiva e na dosimetria da pena, bem como, inclusive, implicar atipicidade da conduta em determinadas hipóteses, independentemente do acordo ou consentimento do usuário. Tais consequências jurídico-penais serão analisadas em Capítulos próprios, sob a ótica da vitimodogmática e do funcionalismo penal.

4.1. Criminologia e os novos aportes da vitimologia

A criminologia é uma ciência criminal autônoma, dotada de método próprio de caráter indutivo, que despontou eminentemente no século XIX em com o escopo de compreender as causas da criminalidade.

A ciência penal dogmática representa uma fração do conhecimento, devendo ser complementada por inflexões interdisciplinares da realidade, cujos aportes são obtidos por meio da criminologia e catalisados pela política criminal.[238] Isso porque a criminologia fornece o "substrato empírico do sistema" que conferirá embasamento às proposições jurídicas do direito penal. A seu turno, a política criminal viabiliza o aglutinamento entre as duas ciências, conectando-as por meio de opções e estratégias concretas a ser desempenhadas pelo Estado.[239] Configura-se, assim, o tripé de sustentação das ciências criminais. Molina e Gomes definem criminologia como:

> Uma ciência (ou uma área de saber, conforme o entendimento) empírica e interdisciplinar, que se ocupa do estudo do crime, da pessoa do infrator, da vítima e do controle social do comportamento delitivo, e que trata de subministrar uma informação válida, contrastada, sobre a gênese, dinâmica e variáveis principais do crime – contemplado este como problema individual e como problema social – assim como sobre os programas de prevenção eficaz do mesmo e técnicas de intervenção positivas no homem delinquente.[240]

Desde a inauguração da criminologia como ciência autônoma, com o advento da escola clássica, o centro gravitacional das investigações foi o criminoso. Pensadores clássicos, como

---

[238] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, p. 53.
[239] SHECAIRA, Sergio Salomão. *Criminologia*. 6. ed. São Paulo: Revista dos Tribunais, 2014, p. 44.
[240] MOLINA, Antonio Garcia-Pablos de; GOMES, Luiz Flávio. *Criminologia*. São Paulo: Revista dos Tribunais, 2002, p. 33.

Rousseau, entendiam que o criminoso, como ser humano dotado de livre-arbítrio, optava voluntariamente pela violação do pacto social. Posteriormente, a escola positivista postulava o criminoso como ser dotado de desvio social atávico, o que se assemelha, portanto, a uma patologia.

Teorias mais recentes continuam a realçar seu protagonismo. Concepções ligadas à criminologia crítica, de viés marxista, buscam apontar o criminoso como objeto e instrumento descartável do modo de produção capitalista. Todas as perspectivas de estudo do infrator não são absolutamente excludentes, mas se completam para constituir um ser histórico, multifacetado e real.[241] Contudo, desvelam uma visão parcial da complexidade do fenômeno delitivo, desenvolvida e aprofundada desde séculos.

A seu turno, a compreensão do outro polo do fenômeno delitivo foi relegada durante significativo período de estudos criminológicos. Isso levou a uma repercussão de quase completo esquecimento da vítima também pelo direito penal. Recentemente, porém, no bojo da criminologia emana a ciência vitimológica, cujo escopo principal reside em problematizar a visão inicialmente simplista acerca do papel da vítima no fenômeno delitivo, de modo a revelar a complexidade de sua compreensão, quer sob a ótica individual, quer em sua inter-relação com o criminoso.[242]

Em razão de sua particular relevância para a compreensão dos crimes informáticos, alguns apontamentos iniciais sobre a visão vitimológica e a classificação da vítima se fazem necessários.

A vitimologia é definida como "ciência criminológica que lida com a vítima do delito, seus elementos, seu papel e, em especial, sua contribuição para o surgimento do delito".[243] Para Jescheck, consiste na ciência que investiga o papel da vítima na gênese do delito, primeiramente, bem como na resolução do conflito causado com o delito, na sequência.[244] Verifica-se contribuição essencial da vitimologia para o conceito de vítima relacional, ou seja, aquela que interage com o autor e o meio. Ademais, as diversas tipologias de vítimas contribuem para a configuração e estruturação dogmática dos tipos penais. [245]

---

[241] SHECAIRA, Sergio Salomão. *Criminologia*. 6. ed. São Paulo: Revista dos Tribunais, 2014, pp. 50-51.
[242] Ibidem, p. 53.
[243] Tradução livre do original: "ein besonderer Zweig entsprossen, der sich mit dem Verbrechensopfer, seinen Merkmalen und seiner Rolle, insbesondere seinem Beitrag zur Verbrechensentstehung, befasst". (EBERT, Udo. Verbrechensbekämpfung durch Opferbestrafung? *Juristenzeitung*, v. 38, n. 17, p. 633-643, 1983, p. 633).
[244] JESCHECK, Hans-Heinrich; WEIGEND, Thomas. *Lehrbuch des Strafrechts*. 4. ed. Berlim: Duncker und Hublot, 1988, p. 41, *apud* SILVA SÁNCHEZ, Jesús María. Innovaciones teórico-prácticas de la Victimología en el Derecho penal. In: *Victimología: VIII Cursos de Verano en San Sebastián = VIII Udako Ikastaroak Donostian.* Universidad del País Vasco/Euskal Herriko Unibertsitatea, pp. 75-83, 1990, p. 77.
[245] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 45.

A vitimologia teve sua origem como forma de resposta à exacerbada vitimização ocorrida na Segunda Guerra Mundial em razão do holocausto nazista. Apesar do resgate do papel desempenhado pela vítima na gênese do crime em meados do século XX, verifica-se que durante vários séculos ela desempenhou um papel secundário dentro da criminologia, do direito penal e processo penal.

Conforme propõe Silva Sánchez, no decorrer da história do direito penal, salvo as tendências vitimológicas das últimas décadas, existiram duas fases distintas quanto ao papel da vítima. Inicialmente, prevalecia o "Direito Penal da Vingança Privada", desde povos primitivos, até alcançar as primeiras fases do direito romano, os povos germânicos, bem como parte do direito medieval. Nessa fase, denominada "idade de ouro da vítima", as reações ao delito competiam ao sujeito passivo, que retribuíam a ofensa, nem sempre proporcional ou talionalmente, sobre o autor ou seus familiares.[246]

Paulatinamente, com o advento do Estado Moderno, o direito penal se consolida como ramo do direito público e, como tal, sob monopólio estatal, que detém com exclusividade o *ius puniendi*. Não há dúvidas de que a publicização do direito penal trouxe diversos avanços no tocante à racionalidade, humanidade das penas e proporcionalidade. Por outro lado, deu ensejo a um longevo período de esquecimento da vítima, cuja voz e interesses restaram relegados ao segundo plano. [247]

Com o decorrer dos séculos, apesar de maior racionalização e humanização das ciências criminais, as vítimas continuaram relegadas a um papel secundário. De fato, como o delito passou a provir de uma relação entre o agente e o Estado, o processo penal se tornou um mecanismo de imposição de sanções (quer por funções retributivas ou preventivas), sem se voltar à reparação do conflito e das relações privadas. Assim, o ofendido se tornou um objeto passivo, alvo do delito. Em verdade, para além de não atender aos interesses da vítima, frequentemente o processo gerava danos adicionais, por meio da vitimização secundária.[248_249]

Com vistas a trazer maior protagonismo à vítima, as primeiras linhas de desenvolvimento da Vitimologia como ciência autônoma da Criminologia ocorreram com Hans

---

[246] SILVA SÁNCHEZ, Jesús María. Innovaciones teórico-prácticas de la Victimología en el Derecho penal. In: *Victimología: VIII Cursos de Verano en San Sebastián = VIII Udako Ikastaroak Donostian*. Universidad del País Vasco/Euskal Herriko Unibertsitatea, pp. 75-83, 1990, p. 77.
[247] Ibidem, p. 78.
[248] Ibidem., p. 165.
[249] Por outro lado, há institutos aptos a conferir maior relevância à vítima no bojo do processo, como a representação do ofendido, iniciativa privada da dação penal face a alguns delitos, e o perdão do ofendido. Recentemente, emerge a justiça restaurativa como mecanismo para conferir maior protagonismo à vítima do delito.

Von Hentig.[250] O termo "vitimologia", a seu turno, foi cunhado com Mendelsohn em 1956, tendo se consolidado academicamente desde então. [251]

Conforme Beristain, o nascimento oficial da Vitimologia sob a perpectiva científica ocorre em 1979, com o Terceiro Simpósio Internacional de Vitimologia.[252] Com o passar dos anos, estudos vitimológicos encontraram guarida na maioria dos países, bem como em organizações internacionais. Neste ponto, merece destaque a Declaração Sobre os Princípios Fundamentais de Justiça para as Vítimas de Delitos e do Abuso de Poder, aprovada em 29 de novembro de 1985 pela Assembleia Geral das Nações Unidas. Nela, restou sedimentada a seguinte definição de vítima:

> As pessoas que, individual e coletivamente tenham sofrido um prejuízo, nomeadamente um atentado à sua integridade física ou mental, um sofrimento de ordem moral, uma perda material, ou um grave atentado aos seus direitos fundamentais, como consequência de atos ou de omissões de violadores das leis penais em vigor num Estado membro, incluindo as que proíbem o abuso do poder.[253]

Trata-se de um conceito dinâmico, apto a se amoldar a mudanças legislativas nos países membros e, por conseguinte, adequada para abarcar novas formas de vitimização, donde provém seu mérito. [254]

A principal contribuição da vitimologia consiste em resgatar a dignidade da vítima no bojo das ciências criminais, reconhecendo-a como um agente autônomo que deve integrar ativamente a compreensão do fenômeno criminal, desde a gênese delitiva até a efetiva execução da pena. Por essa razão, a ciência vitimológica coaduna-se com os valores constitucionais da liberdade e igualdade, ao inserir a vítima em posição paritária quando comparada ao agente da conduta delitiva.

Desde seu início, a vitimologia também trouxe contribuições acerca do perfil de indivíduos que possuem maior predisposição a se tornarem vítimas. Mendelsohn estabeleceu uma classificação de vítimas com base na correlação de responsabilidade para a ocorrência do delito: completamente inocente ou ideal (a qual em nada contribuiu para o delito), vítima de

---

[250] BERISTAIN, Antonio. *Nova criminologia à luz do direito penal e da vitimologia*. Brasília: Editora Universidade de Brasília, 2000, p. 84.
[251] CÁRDENAS, Alvaro E. Márquez. La victimologia como estudio: redescubrimiento de la víctima para el proceso penal. *Revista Prolegómenos. Derechos y Valores De La Facultad De Derecho*, v. 14, n. 27, p. 27-42, 2011, p. 37.
[252] BERISTAIN, Antonio. *Op. cit.*, p. 83.
[253] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Resolução n. 40/34, de 29 de novembro de 1985. *Declaração dos Princípios Básicos de Justiça Relativos às Vítimas da Criminalidade e de Abuso de Poder***,** 1985.
[254] ALEGRÍA, Gíner et al. Aproximación psicológica de la victimología. *Revista derecho y criminología*, n. 1, 2011, p. 29.

culpabilidade reduzida (a qual, por ignorância, se converte em vítima), vítima tão culpável quanto o infrator (provocadora, responsável por sua vitimização) e vítima mais culpável ou unicamente culpável (agressora, que em verdade não pode ser considerada vítima).[255]

Apesar da dificuldade em se estabelecer um critério ontológico de culpabilidade, o que traz problemas insuperáveis a essa classificação, o mérito de Mendelsohn consistiu em já reconhecer a influência do comportamento da vítima sobre a pena cominada ao autor e eventual indenização da vítima.[256]

Em 1948, Von Hentig descreveu treze perfis de vítimas a partir de sua obra "The Crime and his Victim". Para esse autor, indivíduos mais frágeis sob o aspecto biológico ou social são mais suscetíveis a crimes, como crianças, idosos, enfermos mentais e minorias étnicas. Do mesmo modo, estabeleceu classes baseadas no critério psicológico da vítima, como a depressiva, ambiciosa, solitária.[257] Posteriormente, em sua obra "Crime: Causes and Conditions", Von Hentig propõe nova classificação, mais clara, a partir de agrupamentos de quatro critérios[258]: a) impulsos e desinibição;[259] b) resistência reduzida;[260] c) situações da vítima;[261] d) vítima propensa.[262]

Outra relevante classificação é apresentada por Fattah, que, em sua obra "Quelques problemes posés a la justice penale par la victimologie", diferencia as vítimas com base no critério de responsabilidade pela infração: aquelas que não possuem qualquer responsabilidade e outras que são responsáveis em parte.[263] Dentre estas, acerca da predisposição de certos

---

[255] MENDELSOHN, Benjamín. La victimología y las tendencias de la sociedad contemporánea. *ILANUD al día*, v. 4. n. 10, 1981, p. 54-56 *apud* ALEGRÍA, Gíner et al. Aproximación psicológica de la victimología. *Revista derecho y criminología*, n. 1, 2011, p. 39.

[256] CÁRDENAS, Alvaro E. Márquez. La victimologia como estudio: redescubrimiento de la víctima para el proceso penal. *Revista Prolegómenos. Derechos y Valores De La Facultad De Derecho*, v. 14, n. 27, p. 27-42, 2011, pp. 39-40.

[257] Ibidem, pp. 37-38.

[258] Ibidem, pp. 39-40.

[259] Categoria subdividida em: a) ânimo de lucro (movida por enriquecimento fácil, tornando-se vítima de estelionato); b) com vontade de viver (passou um período sem aproveitar a vida, e busca recuperar o tempo perdido e aproveitá-la); c) agressiva (está saturada vitimização, convertendo-se em vitimária); sem valor (a partir de um sentimento de que são inúteis e não possuem valor).

[260] Desdobra-se em: a) estados emocionais ou psíquicos (que influem em seu ânimo e comportamento); b) transições no curso de vida (como inexperiência, puberdade e gravidez); c) perversa (sujeitos desviados explorados); d) viciada (alcoólica); e) depressiva (que nutre sentimento de autodestruição); f) voluntária (permite o ilícito).

[261] Subdivide-se em: a) isolada (afastada de relações sociais); b) por proximidade (familiar, profissional).

[262] Categoria composta pela vítima: a) indefesa (tolera lesão pois persecução judicial causaria mais danos), falsa (autovitimiza para obtenção de alguma vantagem), imune (não sofre com a prática delitiva), hereditária (decorre de reprodução de relações familiares), reincidente (não toma precauções novamente vítima), que se converte em autor (após constante vitimização).

[263] Quanto às vítimas responsáveis, subdividem-se em: a) vítima desejosa ou suplicante; b) vítima consensual; c) vítima sem consentimento, porém favorecedora; d) vítima não participante, que rechaça o ofensor; e) vítima provocativa ou incitadora do criminoso; f) vítima participante, que pode inclusive auxiliar; f) vítima falsa, de suas

indivíduos serem vitimizados, Fattah delineia três critérios aptos a fomentar a predisposição da vítima: a) biopsicológico, em razão da idade, sexo, raça, entre outros fatores; b) social, como condição econômica, profissão desempenhada, locais frequentados; c) psicológico, tais como desvios sexuais, negligência, excesso de confiança.[264]

Merece destaque ainda o estudo de Elías Neuman acerca da Vitimologia, para quem é necessário considerar a facilitação ou provocação da vítima no momento de imposição de pena ao agressor. Para tanto, defende o sopesamento entre a posição social da vítima, o tipo penal tratado, além de aspectos psicossociais que envolvem o delito. Em sua classificação, são relevantes os apontamentos no tocante às vítimas da sociedade, ou seja, setores vulneráveis no seio social aptos a se tornar vítimas e/ou vitimários como crianças abandonadas, idosos, marginalizados socialmente, minorias raciais e pessoas com deficiência.[265]

Beristain também traz à tona o estudo de Sparks, "Research on victims of crime accomplishments", acerca das diversas manifestações de contribuição da vítima para a prática delitiva, notadamente por meio de sua personalidade e das circunstâncias que lhe são próprias. É possível, mediante "negligência ou por excessiva audácia", expor-se a maior risco, ainda que involuntariamente. A seu turno, também exerce relevante papel a vulnerabilidade do indivíduo, tanto em razão de sua situação social, como por força de traços pessoais. No mais, também se destacam as "vítimas atrativas", que atraem o vitimário por meio de seu estilo, de suas atividades diárias, de seu trabalho ou modo de lazer.[266]

Essa evolução na classificação das vítimas mostra-se de alta relevância para os crimes informáticos pois é possível traçar os usuários mais suscetíveis a sofrer ataques, golpes ou ter dados e valores subtraídos no meio virtual. E as classificações tradicionalmente relacionadas fornecem um arcabouço teórico profícuo para se traçar o ponto referencial de perfis vitimais na seara informática. Assim, após traçar as novas propostas criminológicas que guardam estreita relação com a vitimologia nos crimes informáticos (Capítulo seguinte), será feita uma proposta de classificação da vítima no ambiente virtual, tendo por base os perfis tradicionalmente elencados.

---

próprias ações; g) vítima latente ou predisposta. ALEGRÍA, Gíner et al. Aproximación psicológica de la victimología. *Revista derecho y criminología*, n. 1, 2011, p. 43.

[264] BERISTAIN, Antonio. *Nova criminologia à luz do direito penal e da vitimologia*. Brasília: Editora Universidade de Brasília, 2000, p. 97.

[265] ALEGRÍA, Gíner et al. *Op. cit.*, pp. 43-44.

[266] BERISTAIN, Antonio. *Nova criminologia à luz do direito penal e da vitimologia*. Brasília: Editora Universidade de Brasília, 2000, p. 97.

4.2. Criminologia e crimes informáticos

Fixadas as balizas teóricas que cercam a criminologia e a vitimologia, com destaque para o papel central desempenhado pela vítima para a compreensão do genômeno delitivo, busca-se amoldar os entendimentos ditos tradicionais ao ambiente informático. Com isso, será possível compreender o efetivo papel desempenhado pelos usuários para a gênese dos crimes informáticos atinentes a bens jurídicos individuais disponíveis: a autodeterminação informática e o patrimônio.

O estudo de condutas desviantes no ambiente informático tem ensejado discussão sobre o aproveitamento das premissas das teorias criminológicas consolidadas no espaço físico para explicação do fenômeno delinquente virtual. Até o momento, predominam estudos sediados nos Estados Unidos e Grã-Bretanha, embora também incipientes.

Por um lado, há autores que sustentam uma continuidade das teorias criminológicas,[267] por consistirem os crimes informáticos essencialmente em delitos tradicionais executados por meio da tecnologia da informação. Destarte, como a tecnologia seria apenas um instrumento, os elementos dos crimes tradicionais são reproduzidos, tais como aspectos da vitimização: se por um lado, assim como no mundo físico, os usuários informáticos estão cientes de que devem adotar cautelas preventivas mínimas, por outro lado, na hipótese de violação, possuem ciência de que dificilmente haverá recuperação dos bens.[268] Por conseguinte, para essa corrente, sob a ótica criminológica, os crimes informáticos são considerados "vetustos vinhos em novas garrafas".[269] Referido posicionamento merece críticas porquanto excessivamente generalizante, descartando a verificação do surgimento de novos crimes.[270] Seu principal mérito, sem embargo, consiste em incorporar os avanços científicos historicamente sedimentados na seara criminológica, cujo valor não pode ser subestimado.

Em posição diametralmente oposta, surgem autores a sustentar uma ruptura com a criminologia tradicional, pontuando-se que a tecnologia se torna um fator condicionante dos crimes informáticos, principalmente os delitos próprios.[271] O ambiente virtual apresenta características próprias, permeadas pela total ruptura das barreiras geográficas, anonimato e

---

[267] Os principais autores dessa corrente são Susan Brenner e Peter Grabovsky.
[268] GRABOVSKY, Peter N. Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, v. 10, n. 2, pp. 243-249, 2001.
[269] Tradução livre do original: "old wine in new bottles" (GRABOVSKY, Peter N. Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, v. 10, n. 2, pp. 243-249, 2001, *passim*).
[270] FRANÇA, Leandro Ayres. Cibercriminologias. In: FRANÇA, Leandro Ayres; CARLEN, Pat (orgs.). *Criminologias alternativas.* Porto Alegre: Canal Ciências Criminais, pp. 221-249, 2017, p. 224.
[271] Wanda Capeller, Sheila Brown, David Wall são os principais representantes dessa corrente.

possibilidade de afetação instantânea de milhares de pessoas, o que enseja uma reformulação dos estudos criminológicos.[272] Wall defende que não se trata sequer de novo vinho em garrafas novas, mas efetivamente de "novo e vetusto vinho em garrafa alguma."[273]

Conforme pondera França,[274] a melhor postura reside em diferenciar as espécies de crimes cometidos no ambiente virtual. Nesse esteio, em crimes informáticos próprios[275] deve-se reconhecer certo grau de descontinuidade com relação às criminologias tradicionais, buscando-se perspectivas alternativas para a compreensão de práticas inerentes e exclusivas do mundo virtual. De qualquer modo, mais estudos são necessários para se aferir em que medida certas teorias criminológicas podem ser aplicáveis de forma matizada.[276]

D'outra sorte, no tocante a crimes informáticos impróprios,[277] não há óbice para uma incidência da criminologia tradicional, promovidas as necessárias adaptações, por se tratar de condutas já preexistentes ao surgimento da informática, muito embora tenham sido por ela potencializada.[278] No entanto, mesmo diante desses crimes, abre-se espaço para novas teorias criminológicas, em razão de uma frequente simbiose com delito informáticos próprios (empregados frequentemente como crime-meio para a consecução do crime-fim).

Em suma: para os crimes informáticos próprios, surge a necessidade de novas teorias criminológicas para uma adequada compreensão do fenômeno delitivo, sem, contudo, absoluta superação das teorias tradicionais. A seu turno, diante de crimes informáticos impróprios é possível aplicar a criminologia tradicional de forma matizada, permitindo-se a perfusão de novas teorias aptas a compreender o ambiente virtual e traçar paralelos com os crimes informáticos próprios.

Essas matizes da Criminologia tradicional se fazem necessárias principalmente quanto às teorias ecológicas, que exercem grande influência sobre a Criminologia por meio da Escola de Chicago.[279] Isso porque,mormente sob a vertente ecológica dessa corrente criminológica, há notório enfoque sobre a relação do espaço com a criminalidade, de forma que a cidade, por

---

[272] YAR, Majid. *Cybercrime and Society*. 2. ed. London: SAGE, 2013.
[273] Tradução livre do original: "both new and old wine in no bottles" (WALL, D. S. Catching cybercriminals: Policing the Internet. *International Review of Law - Computers & Technology*, v. 12, pp. 201–218, 1998).
[274] FRANÇA, Leandro Ayres. Cibercriminologias. In: FRANÇA, Leandro Ayres; CARLEN, Pat (orgs.). *Criminologias alternativas.* Porto Alegre: Canal Ciências Criminais, pp. 221-249, 2017, p. 240.
[275] Também denominados, nos Estados Unidos, *cyber-dependent crimes.*
[276] Como se verá no capítulo seguinte, muitos estudos são conduzidos indistintamente com relação a crimes informáticos próprios e impróprios. A partir de estudos empíricos, a princípio, há certas características criminológicas aplicáveis a ambas as espécies.
[277] Denominados, segundo criminólogos norte-americanos, cyber-enabled crimes.
[278] FRANÇA, Leandro Ayres. *Op. cit.*, p. 240.
[279] FRANÇA, Leandro Ayres. Cibercriminologias. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em: https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos. Acesso em: 07 out. 2021.

meio de sua disposição físico-espacial, é vislumbrada como essencial para a compreensão do fenômeno delitivo: dado que os núcleos urbanos apresentam maior desorganização, há maior propensão delitiva. Ocorre que, na seara virtual, a noção física de ambiente é pulverizada, tratando-se em verdade de um ambiente descentralizado em que as distâncias são irrelevantes: vigora a omnipresença. De qualquer modo, não se pode olvidar que, embora virtual, a sociedade em rede caracteriza-se como um novo prisma de ambiente: o usuário nele desenvolve sua personalidade e desempenha diversas atividades cotidianas. Logo, a noção virtual de ambiente permite a adoção de devidas adaptações da teoria ecológica.

Ademais, Sydow afasta uma correlação automática entre demais linhas tradicionais da criminologia, [280] porquanto:

A) a teoria da associação diferencial, ao pressupor o aprendizado das práticas delitivas por meio de atividades em grupos, não se coaduna *in totum* com o ambiente virtual, em que os *crackers* também atuam de forma individualizada em seu aprendizado. De qualquer modo, conforme aponta Moura, há interações e grupos de *hackers* em âmbito inclusive global, em que inexperientes passam por processos de imitação e aprendizagem[281];

B) a teoria da anomia parte de premissa de uma reação à normatividade existente, todavia, não se pode atribuir atualmente a existência de uma imposição comportamental rígida no ambiente virtual. A seu turno, é bem verdade que muitos indivíduos vislumbram no anonimato e na obtenção de lucro fácil no ambiente virtual uma oportunidade de mudança de vida econômica, em um cálculo de custo-benefício do sujeito inovador, na concepção de Robert Merton (aquele que aceita os objetivos culturais, porém nega os meios institucionalizados, que agora se expandem ao ambiente virtual). De qualquer modo, referida teoria carece de uma análise global desse cálculo pelo agente, bem como não explica crimes mais sofisticados no ambiente virtual, que nem sempre são frutos de uma disparidade social latente;[282]

C) Não se vislumbra um etiquetamento social dos criminosos informáticos como marginais, afastando-se a teoria conflitiva social do *labelling approach*. Verifica-se, por outro lado, o estereótipo do *hacker* invariavelmente como indivíduo criminoso, de modo a estigmatizá-lo.[283] Isso repercute, a título exemplificativo, na antecipação da resposta penal, tal

[280] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, pp. 636-637.
[281] MOURA, Grégore Moreira de. *Curso de Direito Penal Informático*. Editora D'Plácido: São Paulo, 2021, pp. 73-74.
[282] Ibidem, pp. 92-93.
[283] Ibidem., pp. 101-102.

como materializada no artigo 154-A, parágrafo único, do Código Penal Torna-se essencial, com isso, sua distinção com o *cracker*, verdadeiro agente de diversas práticas delitivas.

Apesar da necessidade de adaptações das teorias criminológicas tradicionais, é imperioso o fomento de novas teorias a fim de se compreender a dinâmica delitiva do ambiente informático. Como discorre Boiteux, é essencial renunciar a mera e desenfreada previsão de tipos penais – além do incremento de penas – tendo em vista a ausência de elementos empíricos a embasar a aptidão do direito penal a prevenir delitos.[284] Assim, as dificuldades encontradas não são superadas pelo recrudescimento penal, na contramão daquilo verificado hodiernamente no ordenamento pátrio. E mais, conduz-se a uma violação ao princípio da intervenção mínima que pauta a dogmática penal no Estado Democrático de Direito.

4.3. Novas propostas criminológicas aos crimes informáticos

O meio ambiente informático apresenta uma peculiaridade: diferentemente do ambiente físico, em que é possível estabelecer mecanismos externos de prevenção de crimes (policiamento, iluminação pública, seguranças particulares, cofres, monitoramento eletrônico), há uma premente necessidade de adoção de medidas de segurança pelos usuários. Afinal, enquanto crimes comuns dependem de uma conjugação espaço-temporal, para crimes informáticos basta a conexão do dispositivo do usuário a uma rede (ou outro dispositivo, *pendrive*, *bluetooth*) a fim de que este se torne uma vítima em potencial. Não há mecanismo perfeito de proteção, em razão de constantes avanços da programação de novos *malwares* e infindáveis esquemas fraudulentos.[285] Disso decorre que a simples interconectividade consiste em um risco a que todos estão submetidos, o que faz jus ao termo "sociedade de risco."

Com isso, o código do ambiente virtual é regido pela assunção de riscos, que podem contar com uma contribuição ativa dos usuários em uma navegação destoante dos padrões de diligência recomendados. O usuário, assim, no exercício do livre desenvolvimento de sua personalidade – quer por meio do bem jurídico-penal autodeterminação informática, quer pela disposição patrimonial no ambiente virtual – é apto a contribuir diretamente para o sucesso da prática de crimes informáticos.

---

[284] BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 12, n. 47, p. 146-187, mar./abr. 2004, p. 158.
[285] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 190.

Em razão da insuficiência das teorias criminológicas tradicionais, outras teorias criminológicas têm recebido forte propulsão internacional no tocante aos crimes informáticos próprios e impróprios. Como denominador comum, essas teorias não abdicam integralmente dos avanços epistemológicos da Criminologia, possuindo certo lastro em concepções ecológicas da Escola de Chicago, devidamente adaptadas ao ambiente virtual. Ainda, todas as teorias reconhecem a centralidade do papel desempenhado pelos usuários para a compreensão do fenômeno delitivo informático. Destarte, trabalha-se com uma relação intrínseca e interdependente entre a criminologia e vitimologia.

São as principais propostas: I) teoria geral do crime (em seu viés vitimológico); II) teoria dos espaços transitoriais; III) teoria das atividades rotineiras; IV) teoria da prevenção situacional do crime. A seguir, será feito um breve escorço acerca dessas teorias, conferindo-se destaque às duas últimas em razão da maior profundidade de estudos e da confluência de suas conclusões ao estudo vitimológico.

Também denominada de teoria do autocontrole, a teoria geral do crime consiste em uma tradicional teoria criminológica voltada aos agentes delitivos. Segundo Gottfredson e Hirchi, indivíduos com baixo autocontrole apresentam maior probabilidade de envolvimento em comportamentos criminosos, posto que impulsivos, impacientes e favoráveis a atividades arriscadas, de forma a desprezar as consequências a longo prazo de seus atos.[286]

A relação entre baixo autocontrole e crimes informáticos é complexa, tendo em vista sua inaplicabilidade aos *crackers* no cometimento de crimes próprios. Em verdade, esses agentes podem até preferir desafios e acesso a dispositivos fortemente protegidos, o que denota maior capacidade calculista.[287] Por outro lado, há de se reconhecer sua aplicabilidade aos crimes informáticos impróprios, que em geral estão relacionados a manobras de engenharia social e, portanto, não pressupõem habilidades técnicas.

Adotando-se a ótica dos usuários e, com isso vitimológica, Gottfredson e Hirchi apontam que o reduzido grau de autocontrole também incrementa as chances de vitimização em crimes tradicionais.[288] De fato, por apresentarem menores níveis de empatia, há prejuízo de sua capacidade de interpretação das intenções daqueles indivíduos com quem se relacionam. Segundo Bossler, há estudos que apontam a incidência dessa lógica também em crimes

---

[286] GOTTFREDSON, M. R. ; HIRSCHI, T. *A general theory of crime*. Stanford, CA: Stanford University Press, 1990.
[287] BOSSLER, Adam. Contributions of criminological theory to the understanding of cybercrime offending and victimization. In: LEUKFELDT, Rutger; HOLT, Thomas J. *The Human Factor of Cybercrime*. New York: Routledge, 2019, p. 43.
[288] GOTTFREDSON, M. R; HIRSCHI, T. *Op. cit.*, p. 17.

informáticos ao priorizar benefícios imediatos em detrimento das consequências futuras. Isso culmina com o envolvimento em atividades online mais arriscadas, como baixar músicas ou pornografia, interação em fóruns e práticas de crimes contra a honra.[289] Com efeito, Pratt *et al* constataram que há significativa associação entre níveis de baixo autocontrole em delitos informáticos nos quais o contato com a vítima é imprescindível, como no *phishing*. [290]

Muito embora não haja unanimidade nas pesquisas internacionais, há uma tendência a se constatar a veracidade dessa correlação em crimes informáticos próprios e impróprios: pessoas com menor nível de autocontrole estiveram mais sujeitas à vitimização por invasão de dispositivo, furto e fraudes na compra de produtos, [291] além de instalação de *malwares.*[292]

Na sequência, Sydow aponta para a relevância da teoria dos espaços transitoriais, a qual, focada na atuação do delinquente, busca traçar paralelos com características psicológicas e habituais.[293] Inaugurada por Karupannan Jaishankar, entende-se que as pessoas introvertidas e que refreiam sua propensão delitiva no mundo físico estão mais sujeitas a cometer crimes informáticos, amparadas pela anonimidade, flexibilização de sua identidade, maior perfusão dos delitos, dificuldade de apuração da autoria delitiva e carência de regulamentações internacionais uniformes.[294]

Dentre as novas propostas apresentadas, essa teoria traz menor enfoque ao papel da vítima, que incide implicitamente sobre a determinação psicológica do autor para a prática do delito. Como se verá, há certa sobreposição entre a teoria dos espaços transitoriais e as demais. No entanto, por abrangerem com maior destaque a vitimologia e serem dotadas de maior adesão doutrinária, será conferida primazia ao desenvolvimento da teoria das atividades rotineiras e da prevenção situacional do crime, evitando-se repetições desnecessárias.

Com vistas a traçar o perfil vitimológico dos usuários do meio virtual, foi desenvolvido significativo número de pesquisas, notadamente nos Estados Unidos, com fundamento na teoria da atividade rotineira ("routine activities theory" ou RAT). Originalmente delineada na área da

---

[289] BOSSLER, Adam. *Op. cit.*, p. 44.
[290] PRATT, T. C. *et al*. Self-control and victimization: A meta-analysis. *Criminology*, v. 52, n.1, pp. 87–116, 2014.
[291] VAN WILSEM, J. Bought it, but never got it: Assessing risk factors for online consumer fraud victimization**.** *European Sociological Review*, v. 29, pp. 168–178, 2013.
[292] HOLT, T. J.; BURRUSS, G. W.; BOSSLER, A. M. Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, v. 62, pp. 1720–1741, 2018.
[293] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 641.
[294] ASSARUT, Nuttapol *et al.* Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. *International Journal of Cybercriminology*, v. 13, n. 1, pp. 84-100, 2019, pp. 86-87.

criminologia ambiental para explicação de crimes tradicionais, teve sua origem com Cohen e Felson.[295]

A premissa estabelecida é a de que a redução da oportunidade do crime conduz a uma queda das taxas de criminalidade, sendo certo que o crime se alimenta de rotinas. Isso porque a maioria dos crimes diariamente praticados é ordinária e com *modus operandi* simples.[296] Assim, há enfoque em curtos trechos de tempo e espaço, privilegiando-se a prevenção secundária.[297]

Há uma conjugação de três condições necessárias para a ocorrência de um crime: um agente provável (1); um alvo (ofendido) adequado (2); e a ausência de um "guardião capaz" potencialmente apto a evitar a prática do crime pelo agente (3). Sem a confluência desses três fatores, a vitimização será reduzida ou eliminada. Dessa proposta se verifica o papel essencial desempenhado pela vítima, que materializa ao menos dois dos três principais elementos para a conformação delitiva.

Classicamente, a definição de um alvo adequado (2) é sintetizada por meio do acrônimo VIVA: valor (pessoas ricas trarão maiores lucros), inércia (propriedades inerentes que permitem maior resistência ao ataque), visibilidade (perceptibilidade pelo agressor) e acessibilidade (habilidade do agressor de contatar seu alvo).[298]

No entendimento de Llinares, a teoria da atividade rotineira confere origem a todas as atuais teorias da oportunidade, adaptando as teorias ecológicas, preeminentemente ambientais. Isso porque essa teoria já visa a se amoldar ao contexto de evolução tecnológica, compreendendo a relevância do incremento do potencial contato entre vítima e vitimário (o que denota um incremento da oportunidade do agressor), com redução de fatores preventivos e o consequente aumento de taxas de criminalidade.[299]

---

[295] COHEN, Lawrence E.; FELSON, Marcus. Social change and crime rate trends: A routine activity approach. *American sociological review*, pp. 588-608, 1979.

[296] WORTLEY, Richard; TOWNSLEY, Michael.Environmental criminology and crime analysis: Situating the theory, analytic approach and application. In: WORTLEY, R. ; TOWNSLEY, M. (eds). *Environmental Criminology and Crime Analysis*, 2. ed. London: Routledge, 2016, p. 90.

[297] Ibidem, pp. 94-95.

[298] Muitos teóricos argumentam que a teoria da atividade rotineita provém da teoria de exposição do estilo de vida, a qual considera como fator relevante para a vitimização as atividades rotineiras, ou seja, o estilo de vida de uma pessoa. (HINDELANG, Michael J.; GOTTFREDSON, Michael R.; GAROFALO, James. *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger, 1978). Com efeito, embora esta teoria busque, em sua origem, explicações demográficas para o risco de vitimização, enquanto a RAT apresenta elementos espaço-temporais, ambas as teorias reconhecem a influência de atividades rotineiras como potencializador de vitimização. (NGO, Fawn T.; PATERNOSTER, Raymond. Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, v. 5, n. 1, 2011, p. 775).

[299] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, *passim.*

Como apontam Leukfeldt e Yar, o emprego da RAT na seara de crimes informáticos obtém guarida por causa de uma série de fatores. Primeiramente, por se tratar de um consenso para análise de diversos crimes tradicionais, como furto, homicídio, furto de veículos e violência doméstica. Ademais, seu esquema analítico de pesquisa permite uma transposição para diversas modalidades de crimes, sendo prescindível um ambiente físico para tanto. Por fim, oferece claros elementos político-criminais para adoção de políticas concretas com vistas à prevenção delitiva.[300] Para Miró Llinares, essa correlação mostra-se efetiva porquanto ressalta a necessidade de adoção de métodos de controles informais, ante a ineficiência do controle formal para o combate à criminalidade informática. Por fim, Wortley e Townsley ressaltam o caráter rotineiro do uso de dispositivos informáticos, justamente a fraqueza que muitos agentes almejam explorar.[301]

Em uma transposição dos elementos da RAT para sua aplicabilidade em crimes informáticos, para se aferir quais vítimas são mais propensas a ataques digitais (análise do alvo adequado), Miró Llinares converte o acrônimo VIVA em IVI, para aglutinar os seguintes fatores: inserção do bem (dados ou valores) no ambiente informático,[302] valor e interação (atuação do usuário no meio virtual perante outros sujeitos e serviços).

No tocante à presença "guardião capaz" (3), investigam-se as possibilidades estruturais e técnicas de os usuários prevenirem ataques. Trata-se de aferir se houve instalação de mecanismos de segurança, como *firewall* e *antimalware* (guardião capaz técnico), além do conhecimento informático dos usuários, acompanhado de consciência dos riscos potenciais na Internet (guardião capaz pessoal).[303]

Nesse esteio, para a compreensão do perfil das vítimas, sob a ótica de adequação do alvo (2) ou ausência de guardião capaz (3), muitos estudos investigam idade, sexo, aspectos financeiros, tempo de permanência do usuário conectado, bem como suas atividades on-line (como em fóruns, redes sociais, lojas virtuais), frequência de acesso a links, anúncios e e-mails desconhecidos (todos esses elementos alusivos ao alvo adequado), bem como existência de *firewalls* e *antimalwares*, além do conhecimento técnico dos usuários (ambos elementos alusivos à existência de "guardião capaz").

---

[300] LEUKFELDT, Eric Rutger; YAR, Majid. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior,* v. 37, n. 3, pp. 263-280, 2016, p. 263.

[301] WORTLEY, Richard; TOWNSLEY, Michael. Environmental criminology and crime analysis: Situating the theory, analytic approach and application. In: WORTLEY, R. ; TOWNSLEY, M. (eds). *Environmental Criminology and Crime Analysis*, 2. ed. London: Routledge, 2016, p. 95.

[302] Uma premissa para se tornar vítima de crimes informáticos consiste justamente em fazer uso dos dispositivos no ambiente virtual. (MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, p. 187).

[303] LEUKFELDT, Eric Rutger; YAR, Majid. *Op. cit.*, p. 270.

Em estudo conduzido em 2016, Leukfeldt e Yar efetuaram extensa investigação com 9161 universitários. No tocante aos crimes informáticos próprios e inserção de *malwares*, constatou-se que a idade desempenha um papel fundamental: quanto mais jovem o usuário, maior o risco. Isso pode ser explicado pelo fato de idosos possuírem maior cautela em razão do limitado conhecimento tecnológico, enquanto jovens insuflam suas efetivas capacidades virtuais. No mais, a renda pessoal também se mostrou proporcional à suscetibilidade de invasão por *malwares*, o que se mostra lógico, tendo em vista a busca por coleta de informações bancárias dos usuários.[304]

No mesmo estudo, concluiu-se que vítimas de invasão de dispositivo informático são mais suscetíveis a ataques conforme sua frequência de navegação em fóruns e redes de relacionamento, o que contribui para maior visibilidade virtual. Do mesmo modo, pessoas com maior consciência acerca dos riscos virtuais estão menos sujeitas a ataques de hacking e fraudes virtuais.[305] Outro fator essencial consiste justamente na frequência de acesso e duração do tempo do usuário conectado à rede: Ashalan[306] aponta relação proporcional entre o lapso temporal do usuário na Internet e sua vitimização por *phishing, hacking*, extorsão e outros delitos.

Choi aponta que há significativa correlação entre o uso de mecanismos de segurança virtuais (*antimalware*, *firewall* e outros) e menor incidência de crimes informáticos e *malware*, sendo um dos principais componentes para redução da vitimização – a reforçar a relevância de um "guardião capaz", segundo a RAT.[307] Ademais, também demonstrou forte relação entre o estilo de navegação online (*online lifestyle*) e maior vitimização, pelo aumento de sua visibilidade. Segundo o autor, usuários que dedicam maior tempo a comportamentos virtuais arriscados, como visita a websites desconhecidos, download de músicas, filmes e imagens são mais suscetíveis a crimes praticados pelo meio virtual, fatores também constatados em estudos realizados por Marcum em 2008.[308]

---

[304] LEUKFELDT, Eric Rutger; YAR, Majid. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, v. 37, n. 3, pp. 263-280, 2016, p. 273.
[305] Ibidem, p. 275.
[306] ALSHALAN, A. *Cybercrime fear and victimization: An Analysis of a National Survey*. Mississipi: Mississipi State University, 2006, p. 123.
[307] CHOI, Kyung-shick. Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, v. 2, n. 1, 2008, pp. 318-319.
[308] MARCUM, C. D. Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, v. 2, n. 2, pp. 346-367, 2008.

É bem verdade que outros estudos apontam resultados inconclusivos no tocante à aplicabilidade da RAT, não exibindo maior incidência de vitimização.[309_310] Ocorre que em geral são constatadas limitações inerentes a essas pesquisas, notadamente no tocante ao número de condutas investigadas (alguns se limitam a uma ou a poucos delitos virtuais, como crimes contra a honra, ameaça, invasão de dispositivo), bem como lastreados em amostras não representativas da população em geral (visto que predominantemente se baseiam em pesquisas junto a alunos universitários) e em amostras de tamanho limitado.[311]

Nesse esteio, apesar de se reconhecer a necessidade de novos estudos para demonstrar precisamente quais fatores vitimológicos se mostram condicionantes na prevenção de condutas nocivas no ambiente virtual, há número suficiente de pesquisas embasadas na teoria da atividade rotineira a apontar a importância da adoção de medidas preventivas mínimas pelas vítimas a fim de coibir delitos informáticos.

Na sequência, Miró Llinares pondera a relevância de técnicas da teoria da prevenção situacional do crime (*situational crime prevention*), devidamente adaptadas às novas tecnologias.[312] Derivada também da teoria da oportunidade, essa teoria lastreia-se na noção de que o criminoso, como ser racional, pondera os custos e benefícios de sua conduta. Nesse esteio, busca-se reduzir as circunstâncias que tornam a prática criminosa atrativa ao agente, notadamente modificando-se as condições ambientais.

Trata-se de uma abordagem criminológica holística, por meio da qual se conclui que a prática de crimes ocorre a partir da ponderação entre custos e benefícios pelo agente. Destarte, busca-se influenciar o comportamento do agente por meio do incremento de custos e redução dos benefícios da prática delitiva.[313]

Sua atuação é majoritariamente focada na prevenção secundária, verificando-se elementos sólidos a amparar a teoria nos crimes tradicionais, como por meio do aumento de vigilância e iluminação em locais públicos. Cornish e Clarke traçam cinco categorias reitoras para influir sobre o cálculo do agente: a) aumento do esforço para a prática delitiva (ao tornar a prática mais dificultosa e onerosa), b) incremento dos riscos (aumentar probabilidades de

---

[309] BOSSLER, A. M.; HOLT, T. J. The Effect of self-control on victimization in the cyberworld**.** *Journal of Criminal Justice*, v. 38, pp. 227-236, 2010.

[310] NGO, Fawn T.; PATERNOSTER, Raymond. Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, v. 5, n. 1, 2011.

[311] LEUKFELDT, Eric Rutger; YAR, Majid. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, v. 37, n. 3, pp. 263-280, 2016, p. 264.

[312] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, pp. 200-202.

[313] BEEBE, Nicole Lang; RAO, V. Srinivasan. Using situational crime prevention theory to explain the effectiveness of information systems security. In: *Proceedings of the 2005 SoftWars Conference***,** Las Vegas, NV, pp. 1-18, 2005, p. 2.

apuração de autoria), c) redução dos ganhos (obstar lucros vultosos), d) redução dos incentivos/provocações (aspecto emocional e psicológico do criminoso); e) eliminação de pretextos (alegada falta de ciência de ilicitude ou imoralidade dos agentes). [314]

Por outro lado, pela própria natureza difusa e descentralizada do ambiente virtual, torna-se desafiador influir sobre o cálculo do ofensor nos crimes informáticos: os riscos parecem relativamente baixos (acobertados pelo anonimato e dificuldades investigativas), enquanto os benefícios, inúmeros (possibilidade de afetação de inúmeros usuários).[315]

Apesar das limitações de uma aplicação imediata das teorias ecológicas, a que pertence a prevenção situacional do crime, não se pode olvidar que o ciberespaço consiste em um novo ambiente, em que a lógica de desorganização e o reduzido controle social (formal e informal), igualmente, criam condições aptas ao desenvolvimento da criminalidade. Partindo-se da premissa de que as características do ambiente condicionam a prática delitiva, verifica-se que a virtualidade – dotada de individualismo, omnipresença e dificuldade de apuração de autoria –, de fato, propicia a criminalidade, o que enseja, *a contrario sensu*, a busca por intervenções para redução das oportunidades delitivas em rede.[316]

Miró Llinares destaca ainda que a plasticidade do ambiente virtual, por este ainda se encontrar em constante atualização e expansão, viabiliza que seja projetado futuramente com viés preventivo, como nas políticas de segurança de softwares e sites.[317]

Amoldando os entendimentos da teoria clássica, porém reconhecendo as peculiaridades do ambiente virtual, Miró Llinares propõe na teoria situacional do crime: a) a supressão da categoria referente à redução de incentivos/provocações, porquanto ausente conexão física ou emocional com a vítima na seara virtual; b) a inclusão da categoria denominada redução do âmbito de incidência, em que a vítima reduz seu âmbito de exposição virtual, prevenindo ataques e a conversão de seu dispositivo em "zumbi", o que também repercutirá em aumento do esforço pelo agente.[318]

De início, para a redução do âmbito de incidência, em adesão à teoria proposta por Llinares, Agustina sugere a educação digital. Propõe a supervisão das atividades de crianças e

---

[314] CORNISH, D.V.; CLARKE, R.V. Oportunities, precipitator and criminal decisions. A reply to Wrtley's citique of situational crime prevention. In: SMITH, M.; CORNISH, D. B. (coords.). *Theory for Practice in Situational Crime Prevention*, v. 16, New York, Monsey: Criminal Justice Press, 2003.
[315] BREWER, Russell et al. *Cybercrime prevention: Theory and applications*. Springer Nature, 2019, p. 43.
[316] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, pp. 203.
[317] Ibidem, p. 204.
[318] Ibidem, pp. 206-207.

adolescente, assim como a conscientização dos usuários com relação ao fornecimento de dados pessoais, como a localização revelada em redes sociais.[319]

Autores como Luiz D'Urso suscitam a necessidade de adoção de uma disciplina específica em escolas no ensino fundamental e médio, a fim de que os jovens adquiram ciência dos riscos do ambiente digital. Isso repercutirá, a médio e longo prazo, em uma redução da vitimização em todas as faixas populacionais.[320]

Esse mecanismo se torna o principal responsável pela reversão do perfil da vítima ignorante sob o prisma informático, ensinando o titular do bem jurídico a valorizá-lo, evitando exposições a riscos supérfluos. Ademais, enseja-se reflexão a todos os usuários, potencialmente enquadráveis como vítimas solitárias, gananciosas e curiosas em algum momento de suas atividades virtuais. Afinal, como pondera Sydow, significativa parcela dos ataques pode ser coibida por meio da identificação dos métodos de ação dos agentes e de seus objetivos. [321]

Com efeito, o enfoque na adoção de estratégias preventivas de educação dos usuários (técnica de prevenção social primária do delito) se mostra mais profícua do que conferir ao Direito Penal o papel primordial por meio da repressão. Como reiteradamente se verifica, ao se conferir demasiado protagonismo às leis penais, emerge uma tendência punitivista, o que não se coaduna com o Estado Democrático de Direito. Isso não significa, por outro lado, o abandono da seara penal, mas sua aplicação à luz do princípio da intervenção mínima.

Torna-se evidente o papel de destaque desempenhado pelos usuários no ambiente virtual, o que denota marcante aspecto vitimológico da teoria da prevenção situacional do crime. Afinal, a atuação diligente do usuário em rede consiste no método mais simples e direto para incremento da relação custo-benefício da prática delitiva.

Nessa linha, a fim de se aumentar o esforço percebido pelo ofensor, Miró Llinares traz cautelas a serem adotadas pelos usuários, como instalação de *firewalls*, antivírus, constante atualização do sistema informático e das senhas adotadas, o que viabiliza controle de acesso ao sistema e rápida detecção de ataques.[322]

---

[319] AGUSTINA, Jose R. Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, v. 9, n. 1, 2015, pp. 47-48.

[320] D'URSO, Luiz Augusto Filizzola. Crimes praticados pelas redes sociais: Induzimento ao suicídio, à autolesão corporal e os crimes contra a honra. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em: https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos. Acesso em: 16 ago. 2021.

[321] SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 694.

[322] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, p. 208.

A atuação dos usuários, por outro lado, deve ser conjugada a outros fatores preventivos, como a célere a retirada dos agentes desse ambiente, com o encerramento de *websites* maliciosos, retirada de conteúdo ilícito, mecanismos eficientes de denúncia.

Deve-se pontuar também a necessidade de transferência de parte da responsabilidade pela proteção dos dispositivos às próprias plataformas operacionais, como Windows, Apple, Android e iOS. Muito embora atualmente haja maior proporção de crimes informáticos próprios em face de dispositivos Windows/Android (em celulares), isso se deve em parte ao fato de ser o sistema globalmente predominante.[323]

Para o incremento do risco percebido pelo agente, Agustina sugere acréscimo do número de guardiões capazes (na linha da proposta da teoria da atividade rotineira), como a infiltração de agentes e vigilância por equipes policiais especializadas em crimes virtuais.[324_325]

Miró Llinares expõe a necessidade de incremento de moderadores em fóruns e na própria rede, especialmente na *darkweb*, além da redução do anonimato, de modo a se facilitar célere identificação do IP do qual originada a contuda ilícita.[326]

Em nosso país, tivemos avanços com o Marco Civil da Internet, porém ainda são necessários aprimoramentos. De início, é imprescindível o aumento do lapso temporal em que os provedores de conexão e de aplicação são obrigados a manter dados do usuário atualmente em tempo extremamente exíguo, de seis meses e um ano, respectivamente, nos termos dos artigos 13 e 15, do Marco Civil da Internet. Isso culminaria com uma redução da sensação de anonimato no ambiente virtual, posto que a permanência do armazenamento de dados por longo período viabilizaria investigações de delitos praticados em anos anteriores.

Atualmente, a responsabilização subsidiária do provedor de Internet somente após notificação judicial (artigo 21, do Marco Civil da Internet) não traz incentivos de aprimoramento das plataformas. Ademais, voltam-se tão somente à remoção de conteúdos de

---

[323] Com efeito, apesar de o sistema Apple ser tecnicamente superior, em regra, viabilizando maior proteção, a tendência é de crescimento e pulverização de novos *malwares* a quaisquer dispositivos, inclusive voltados a aparelhos celulares de última geração e outros dispositivos que compõem a IOT (*Internet of Things*). Referida realidade enseja, igualmente, aprimoramento de *firewalls*, *antimalware*s e antivírus pelas respectivas plataformas, sob pena de imputação de responsabilidade às empresas nas esferas civil e administrativa. (WILLEMS, Eddy. *Cyberdanger: Understanding and Guarding Against Cybercrime*. Springer, 2019, p. 187).

[324] AGUSTINA, Jose R. Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, v. 9, n. 1, 2015, p. 48.

[325] WILLEMS, Eddy. *Op. cit.*, p. 174. Willems faz menção ao êxito dos denominados *professional cybercrime hunters*, ou "caçadores profissionais de crimes informáticos", que acompanham as ameaças virtuais cotidianamente e rapidamente respondem a violações de segurança de redes e dispositivos, além de atuar na prevenção de ataques. Nos Estados Unidos, são denominados CERTS (Computer Emergency Response Teams), enquanto na Europa há um corpo transnacional e integrado de proteção virtual, alcunhado ENISA (European Agency for Network and Information Security Agency).

[326] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, pp. 208-209.

cunho sexual, excluindo-se uma vasta gama de delitos informáticos, que apenas ensejam responsabilização após descumprimento de ordem judicial específica (artigo 19, do Marco Civil da Internet). Logo, mostra-se imperioso o incremento legislativo, a fim de que as plataformas (como redes sociais) se tornem civil e administrativamente responsáveis por demais conteúdos ilícitos transmitidos, independentemente de interpelação judicial.[327]

Referidas modificações estruturais podem ser aptas a iniciar um processo de reversão do pensamento de que não há consequências ou regulamentação aos usuários, mitigando-se a perspectiva de diluição de meios de controle formal.[328]

Com vistas a reduzir os ganhos auferidos pelo agente, é viável a utilização de sistemas de blockchain e criptografia, armazenamento de dados em *hardwares* não conectados ao dispositivo, uso de sistemas de pagamento seguros (como *Paypal*), aperfeiçoamento dos sistemas de e-commerce e bancários. Ainda, é necessária uma persecução penal célere, também ampliada à criminalidade organizada e delitos de lavagem de dinheiro.[329]

Por fim, para se eliminar pretextos dos agentes, Agustina propõe a adoção de políticas digitais em empresas e no setor público cumulado com um compliance efetivo.[330] Trata-se de processo de exteriorização e conscientização de condutas criminais no ambiente virtual, de modo que atividades ilegais praticadas no ambiente de trabalho devem ser levadas ao conhecimento da autoridade competente.[331] Outro mecanismo consiste no envio de avisos aos agentes acerca da existência de licenças, políticas de privacidade e conscientização dos agentes sobre o comportamento adequado virtual.[332] Sugere-se, ainda, o incentivo a competições legais de hackers, além de sua contratação para emprego de seu conhecimento em locais adequados.[333]

---

[327] D'URSO, Luiz Augusto Filizzola. Crimes praticados pelas redes sociais: Induzimento ao suicídio, à autolesão corporal e os crimes contra a honra. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em: https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos. Acesso em: 16 ago. 2021.

[328] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, pp. 188.

[329] Ibidem, p. 208-209.

[330] AGUSTINA, Jose R. Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, v. 9, n. 1, 2015, p. 48.

[331] LEUKFELDT, Rutger; JANSEN, Jurjen. Financial cybercrimes and situational crime prevention. In: LEUKFELDT, Rutger; HOLT, Thomas J. *The Human Factor of Cybercrime*. New York: Routledge, 2019, p. 233.

[332] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, pp. 208.

[333] KRANENBARG, Marleen Weulen. Contrasting cyber-dependent and traditional offenders: a comparison on criminological explanation and potential prevention methods. In: LEUKFELDT, Rutger; HOLT, Thomas J. *The Human Factor of Cybercrime*. New York : Routledge, 2019, pp. 207-208.

Na hipótese de identificação do autor de delitos informáticos, a implementação da justiça restaurativa consiste em uma alternativa a ser considerada, com vistas a personificar as vítimas perante o agressor, aumentando sua conscientização.[334]

Em se tratando de controle formal, a principal estratégia reside na harmonização internacional do direito na seara informática, uniformizando-se os delitos, a persecução penal, mas também a regulamentação do tráfego de dados e a proteção de dados pessoais, com construção de um modelo de repressão e em âmbito internacional, inclusive com um sistema de jurisdição universal. [335]

Das teorias criminológicas atualmente voltadas aos delitos informáticos, depreende-se papel de destaque conferido sobre a vítima do delito, emergindo a relevância da vitimologia. A teoria geral do crime traz indicativos de que ofendidos com menor autocontrole são mais suscetíveis a crimes virtuais. Do mesmo modo, a teoria das atividades rotineiras revela diversos comportamentos de usuários influem decisivamente sobre a vitimização, notadamente a manutenção de *antimalwares* e *firewalls*, conhecimentos informáticos básicos e a prática de atividades arriscadas. Em complemento, a teoria da prevenção situacional do crime traz à baila papéis essenciais do usuário, sem deixar de ser amparado por políticas públicas e legislativas adequadas. Logo, torna-se uníssona em todas essas teorias a imprescindibilidade do papel protagonista do usuário, a ser propulsionado pela promoção de uma educação digital adequada.

4.3.1. Caminho constitucional e garantista para o papel da vítima nos crimes informáticos

As vertentes criminológicas preexistentes não se mostram aptas a fazer frente à completude do fenômeno delitivo informático. No entanto, suas contribuições não podem ser descartadas, mas assimiladas com adaptações. Na atualidade, recebem grande adesão a teoria geral do crime sob o viés vitimológico e as teorias dos espaços transitoriais, da prevenção situacional do crime e a da atividade rotineira. Todas apresentam intersecções e destacam as especificidades do novo ambiente. Ao nosso sentir, a teoria dos espaços transitoriais apresenta maior número de limitações, posto que excessivamente focada na compreensão do delinquente, abstraindo-se demais fatores relevantes – notadamente, a vítima. Ainda, a teoria geral do crime,

---

[334] BREWER, Russell et al. *Cybercrime prevention: Theory and applications*. Springer Nature, 2019, pp. 117-118.
[335] Schünemann traz à baila preocupações pertinentes acerca da adoção de um processo penal transnacional, que em geral culmina com um sistema de justiça criminal mais punitivo, ferindo o equilíbrio processual. Dessa forma, não se deve priorizar uma uniformização internacional em detrimento de princípios penais basilares, de modo que essa estratégia não se mostra profícua isoladamente e deve ser implementada à luz do modelo de Estado Democrático de Direito. (SCHÜNEMANN, Bernd. As bases do processo penal transnacional. *Revista Brasileira de Ciências Criminais.* São Paulo, v. 19, n. 90, p. 189-209, mai/jun. 2011, p. 191).

reformulada para se dirigir à análise do autocontrole da própria vítima, também traz uma explicação parcial ao fenômeno delitivo. A seus turnos, as teorias da prevenção situacional do crime e a da atividade rotineira mostram-se profícuas a traçar linhas de estudos criminológicos futuros. Seus aspectos são complementares, e várias de suas categorias, intercambiáveis.

Notório denominador comum consiste em conferir um papel protagonista aos usuários (e potenciais vítimas) na gênese do fenômeno criminoso. Trata-se da consequência do individualismo em rede, em que o usuário atua preponderantemente de forma singular, contruindo sua sociabilidade em redes por ele previamente selecionadas, com base em seus gostos ou necessidades, em um aprofundamento da tendência individualista já inserida na estrutura social dominante. [336]

Tal protagonismo deflui igualmente do valor constitucional do livre desenvolvimento do indivíduo, o que perpassa pelo reconhecimento de suas responsabilidades na sociedade atual. A assunção de riscos no ambiente virtual torna-se um dos prismas da manifestação da liberdade de atuação do usuário, o que implica reconhecer que atos de disposição ou exposição ativa do bem jurídico disponível são práticas de desenvolvimento da personalidade em uma sociedade em rede e de risco. E isso deve trazer repercussões penais, porque, como visto neste Capítulo, criminologicamente verifica-se uma relação causal entre as condutas adotadas pelos usuários e o incremento de práticas delitivas.

Referida realidade conduz à necessidade de empoderamento dos atuantes, quebrando-se o paradigma de mera sociedade de espetáculo, tendo em vista que todos os agentes contribuem para a formação da Internet. Isso ocorre por uma simples navegação, um *post* em rede social, curtidas, registros em fóruns: se deixamos nossos rastros digitais (*digital footprints*), igualmente integramos o ambiente informático.

Considerando que a simples presença do usuário no ambiente virtual já permite maior correlação de vitimização, bem como que há crescente tendência de incremento na duração do uso diário de dispositivos informáticos em decorrência do individualismo em rede, enseja-se uma prevenção focada especificamente na formação e educação digital dos usuários.[337]

Como aponta Willems, com o aprimoramento de mecanismos de defesa e bloqueios a *malwares* (além do sucesso da adoção de outras medidas preventivas), haverá tendência de proliferação de práticas de engenharia social, voltando-se ao elo mais fraco da corrente: o

---

[336] CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006, p. 24.
[337] MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012, pp. 269.

usuário.[338] Sem sua cooperação, inexistem mecanismos de proteção fática ou jurídica. Isso porque a via alternativa consiste em um incremento de vigilância e redução das liberdades em rede, preço que a sociedade não pode estar disposta a pagar, sob pena de desvirtuamento do Estado Democrático de Direito.

Para Agustina, a tensão entre liberdade e segurança é o dilema central no ambiente virtual: com maior liberdade de navegação, sem rigoroso controle e regido pela anonimidade, em regra, deve-se tolerar o inevitável surgimento de novas oportunidades criminais. Apesar de propostas de vigilância, as sociedades modernas não irão impor a segurança virtual a todo custo, o que implica a importância de enfoque na prevenção dos riscos direcionada às vítimas. [339]

Como visto, no entanto, referida realidade não implica desamparo aos usuários, responsabilizando-os por quaisquer condutas adotadas no ambiente virtual. Não há dúvidas de que, pela própria individualização do uso dos dispositivos e natureza pulverizada da Internet, à vítima incumbirá o papel protagonista na prevenção delitiva, de modo a atuar precipuamente no nível de prevenção secundária. Sem embargo, não se pode imputar-lhe o ônus preventivo de forma exclusiva, o que importaria em indevida responsabilização dos usuários. De se ponderar, nesse contexto, medidas paralelas de atuação, além de políticas que visem a auxiliar o usuário em sua proteção e tomadas de decisão no ambiente virtual, conforme delineado quando do estudo da teoria a prevenção situacional do crime.

A harmonização dos tipos penais, a cooperação investigativa e a persecução penal global são um caminho necessário e inevitável. Contudo, deve-se atentar aos perigos que cercam essa tendência regulamentadora e punitivista. Seus reflexos já são percebidos em nosso ordenamento pátrio, em que efetuadas alterações pontuais por meio da Lei n. 14.155/2021, com recrudescimento penal demagógico, sem a necessária articulação dos setores envolvidos em âmbito nacional e mundial. Já apontava Galán Muñoz há mais de uma década:

> Seria possível dizer, portanto, sem temor de nos equivocarmos que nesse âmbito concreto, no direito penal informático internacional, o binômio prevenção-repressão está vencendo novamente aquele outro que se conforma pela união de garantias e liberdades.[340]

---

[338] WILLEMS, Eddy. *Cyberdanger: Understanding and Guarding Against Cybercrime*. Springer, 2019, p. 188.

[339] AGUSTINA, Jose R. Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, v. 9, n. 1, 2015, p. 37.

[340] Tradução livre do original: "Se podría decir, por tanto, sin demasiado temor a equivocarnos que en este concreto ámbito, en el Derecho penal informático internacional, el binomio prevención-represión está venciendo de nuevo a aquel outro que se conforma por la unión de garantías y libertades." (GALÁN MUÑOZ, Alfonso. Mitos y realidades de la delincuencia informática. Un estudio sobre la reforma del Código Penal brasileño en materia de delitos informáticos, a la luz del Derecho penal Internacional. *Revista justiça e sistema criminal: modernas tendências do sistema criminal*, Curitiba, v. 1, n. 1, pp. 57-98, jul./dez. 2009, p. 94. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=89162. Acesso em: 22 jul. 2021).

Por outro lado, a jurisprudência pátria, na seara consumerista, já vem reconhecendo a relevância da adoção de cautelas mínimas pelos usuários, afastando-se indenizações diante da desídia da vítima. Com isso, o Tribunal de Justiça de São Paulo negou o reconhecimento de falha de prestação de serviços bancários em face de vítima que pagou boleto falso alusivo ao refinanciamento de dívida encaminhado via Whatsapp. Isso porque incumbe ao autor adotar medidas básicas para aferir a legitimidade do contato efetuado por aplicativos de mensagens, em circunstâncias completamente canhestras àquelas que costumam ocorrer para a renegociação de dívidas.[341] Destarte, não se reconhece direito à indenização em face da instituição financeira. Se, por um lado, não se está diante de pleito de indenização diretamente em face do indivíduo responsável pela fraude, por outro, é de se pontuar a perfusão no ordenamento jurídico da necessidade de adoção de cautelas no ambiente virtual, inclusive sob a ótica protetiva ao consumidor. Com mais, razão, deve haver sua materialização na seara penal, em que preponderam os princípios da fragmentariedade, subsidiariedade e ofensividade.

Destarte, em prol da consecução de um Direito Penal Informático Mínimo – calcado no princípio da intervenção mínima –, bem como em observância aos postulados de liberdade e livre desenvolvimento do indivíduo, inerentes ao Estado Democrático de Direito, inarredável a adoção de um papel protagonista pela vítima na prevenção de crimes informáticos, o que, evidentemente, trará implicações relevantes sobre a teoria geral do delito.

4.3.2. Atitudes preventivas da vítima nos crimes informáticos

As teorias criminológicas emergentes apontam para uma necessária conscientização dos usuários como fator chave para a prevenção delitiva. Apesar de todos os usuários conectados estarem sujeitos a delitos informáticos, sua imensa maioria pode ser evitada a partir de um comportamento cauteloso básico do titular do dispositivo. Assim, uma exposição ativa e autônoma a riscos informáticos passa a ser depreendida, em verdade, como manifestação do próprio desenvolvimento da personalidade do indivíduo no ambiente digital.

Por um lado, são proporcionalmente pouco frequentes ataques perpetrados por *crackers* de forma direcionada, situações normalmente restritas a grandes empresas, órgãos públicos e

[341] Tribunal de Justiça de São Paulo. Apelação Cível n. 1012542-19.2021.8.26.0577, 23ª Câmara de Direito Privado, relator Hélio Nogueira, julgado em 20 out. 2021. Apelação Cível n. 1054914-30.2019.8.26.0002, 11ª Câmara de Direito Privado, Relator. Marco Fábio Morsello, julgado em 27 jul. 2020. Apelação Cível n. 1003235-49.2019.8.26.0597, 14ª Câmara de Direito Privado, Relator Thiago de Siqueira, julgado em 12 dez. 2019.

pessoas políticas. Nessas hipóteses, visto que concernentes a agentes com elevada capacidade técnico-informática, não há formas de prevenção suficientes para usuários leigos.[342]

No entanto, todas as demais condutas lesivas praticadas no meio informático – que respondem pela maioria dos delitos informáticos - dependem de algum grau de colaboração da vítima. A prática de engenharia social pressupõe, em regra, conhecimentos informáticos básicos, lastreando seu sucesso na habilidade de criar aparência verídica à fraude, ao ardil elaborado. Trata-se de explorar alguma fragilidade ou a ingenuidade da vítima, por medo, curiosidade, ganância e outros fatores psicológicos. Logo, com algum grau de negligência da vítima os agentes obtêm acesso a dados ou valores, podendo culminar com a prática de furto mediante fraude, estelionato e outros delitos.

Ademais, é muito frequente o emprego de anúncios, links e e-mails fraudulentos que induzem a vítima a instalar, involuntariamente, *malwares* em seu dispositivo informático. Por outro lado, sempre há uma escolha expressa da vítima, ainda que mediante engano: um clique em um link, anuência com um download, o que acaba por ocasionar a contaminação do dispositivo. São condutas que, por si, nem sequer configuram crime, como visto no Capítulo 3.4.1.1. (Condutas lesivas atualmente abarcadas pelo artigo 154-A, caput, com a redação dada pela Lei n. 14.155/2021), podendo culminar, tão somente, com delitos informáticos impróprios stricto sensu ou mediatos, a depender da finalidade do agente.

Nesse esteio, considerando a correlação direta entre a fragilidade do usuário e maior suscetibilidade a crimes informáticos, impõe-se a promoção de sua educação digital, com vistas a uniformizar deveres de cautela como forma de reduzir sensivelmente as práticas nocivas no meio virtual.

Mostra-se de magna pertinência a adoção de medidas de proteção do dispositivo (guardião capaz, para a teoria das atividades rotineiras), que podem ser sintetizadas em: a) atualização constante do sistema operacional e navegadores da web, de modo a corrigir eventuais falhas de segurança descobertas por *crackers*; b) instalação, ativação e atualização de *firewall* e *antimalwares* (notadamente antivírus e *antimalware*).[343] De pouca valia é a manutenção desses mecanismos sem sua devida atualização e ativação, o que torna o dispositivo muito mais suscetível a ataques.[344]

---

[342] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, p. 191-193.

[343] CASSANTI, Moisés de Oliveira. *Crimes virtuais, vítimas reais*. Rio de Janeiro: Brasport, 2014, pp. 42-43.

[344] A sociedade em rede, de velocidade, leva os usuários a uma mentalidade de início imediato, sem o aguardo de processos para a devida desativação e atualização, sendo usual que o dispositivo não seja efetivamente desligado, mas permaneça apenas em modo de suspensão de atividade. Ocorre que isso obsta a instalação de atualizações no

Uma configuração adequada do dispositivo mitiga as chances de instalação de *malware*. No entanto, é necessária constante cautela durante navegação, evitando-se clicar em links e ingressar em sites de procedência desconhecida. Caso a URL se inicie com "HTTPS", o acesso será confiável, devendo-se priorizar o acesso a esses sites. Anúncios sensacionalistas, que fazem menção a prêmios surreais instantâneos ou mesmo insistem na mensagem "clique aqui", consistem em clássicas modalidades de infecção de dispositivos por *malware*.[345] Outra conduta prudente consiste em evitar digitar quaisquer dados pessoais em computadores públicos, equipamentos de terceiros (Cafés, lanhouses) ou redes públicas de *wi-fi*.[346]

Para se prevenir ataques de força bruta, é imprescindível a adoção de senhas sólidas. Ocorre que, conforme pesquisas, usuários insistem em utilizar senhas simples e frágeis, como password ("senha" em inglês), sequências numéricas como 123456, a palavra "senha". Além dessas, são muito frequentes padrões numéricos baseados em data de nascimento de parentes ou seus nomes.

As práticas de *phishing* apresentam ampla variedade a fim de ludibriar vítimas. Inicialmente, para se evitar websites falsos de instituições financeiras, é necessário verificar se se trata da página oficial – que sempre apresentará HTTPS.[347] O usuário deve sempre digitar a URL, evitando clicar em links, emails e anúncios. Do mesmo modo, é prudente sempre efetuar o log-off do usuário, clicando no botão "sair". É exaustivamente repetido pelas instituições a ausência de telefonemas e e-mails requerendo a senha pessoal e chave de segurança do correntista, nunca devendo fornecê-los a terceiros.

Atualmente não há limites para compras de bens e serviços pela Internet, o que enseja a multiplicação de *websites* falsos, que capturam dados e, frequentemente, valores transferidos pelas vítimas na expectativa de receber certo produto. Deve-se desconfiar de sites que vendam produtos a preço muito inferior ao mercado, sendo recomendada prévia consulta a sites de proteção do consumidor, como o "Reclame Aqui" (reclameaqui.com.br) e Procon. Trata-se de sites falsos que vendem produtos eletrônicos (mais atraentes aos consumidores), sites de leilão, jogos de azar manipulados. Em aquisição junto a particulares, é imprescindível prévia verificação dos dados e avaliações do vendedor, encontrada em sites confiáveis como "Mercado Livre."

---

dispositivo, sendo recomendável, sempre que possível, desligá-lo completamente. (WILLEMS, Eddy. *Cyberdanger: Understanding and Guarding Against Cybercrime*. Springer, 2019, p. 86).

[345] CASSANTI, Moisés de Oliveira. *Crimes virtuais, vítimas reais. Op. cit.*, p. 50.

[346] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 86.

[347] CASSANTI, Moisés de Oliveira. *Crimes virtuais, vítimas reais*. Rio de Janeiro: Brasport, 2014, p. 48.

Por fim, exige-se redobrada cautela com relação a anúncios e e-mails, principais instrumentos para prática de engenharia social. Normalmente, há persuasão de fornecimento de dados ou valores mediante exploração da ingenuidade da vítima, quer por medo (dívidas vencidas, encerramento de contas bancárias, execuções junto ao Poder Judiciário), curiosidade (acesso a vídeos de caráter erótico, acidentes, que também podem levar à instalação de *malwares*) ou ganância (recebimento de herança de parente desconhecido, vencedor em premiação ou sorteio, promoção de produtos). É necessário sempre desconfiar de mensagens desse teor, provindas de remetentes desconhecidos e inclusive de pessoas conhecidas – que podem ser infectadas por *malwares* -, sendo frequentes ainda erros gramaticais e afirmações genéricas.[348] Também se mostra frequente a prática de fraude mediante sites e aplicativos de relacionamento, em que um indivíduo geralmente se aproxima e, mediante engodo, induz o terceiro a fornecer dados pessoais ou mesmo valores.[349]

Por fim, impõe-se prudência dos usuários com seus arquivos armazenados, de modo a sempre guardar um *back-up* em outros dispositivos (como *pendrive* ou *HD*). Assim, caso sofra um ataque informático, suas consequências serão mitigadas.

O simples fato de o usuário navegar em rede informática impõe-lhe uma série de deveres de cautela, de forma a prevenir e mitigar danos a que inexoravelmente está sujeito. Na atualidade, o meio ambiente virtual é aquele mais emblemático da sociedade de risco, posto que vincula, simultânea e constantemente, bilhões de indivíduos em todo o mundo. Em que pesem esforços governamentais, de ONGs e empresas em combate aos *crackers*, sobre o indivíduo, titular de seu dispositivo, sempre recairão os principais mecanismos de prevenção de práticas nocivas.

4.4. Proposta de classificação das vítimas informáticas

A era digital trouxe uma velocidade inusual, acompanhada de uma exacerbação do individualismo. No entendimento de Castells, culmina-se com tendência de desfragmentação da própria personalidade: em razão das diferentes máscaras e feições adotadas no ambiente virtual, torna-se difícil distinguir o ego real de seu ego digital.[350] Essa linha é tênue e

[348] CASSANTI, Moisés de Oliveira. *Crimes virtuais, vítimas reais*. Rio de Janeiro: Brasport, 2014, pp. 51-52.
[349] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, p. 85.
[350] CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roneide Venancio Majer. V.1. 6. ed. São Paulo: Paz e Terra, 2011, pp. 38-40.

frequentemente pouco clara, como em casos de adolescentes que permanecem horas a fio em frente ao computador, lá desenvolvendo suas características relacionais.

Assim, essa cisão entre mundo real e virtual é colocada em xeque, sendo que ambos são parte efetiva da realidade, verificando-se uma fusão de identidade entre o ser humano e o dispositivo informático: o ego criado no ambiente virtual ao mesmo tempo possui personificação distinta do físico, porém também integra e compõe a realidade.[351]

É nesse contexto que ganha relevância o denominado efeito desinibidor. No ambiente virtual, surgem tendências de maior impulsividade, confiança e ingenuidade, em que os indivíduos adotam condutas que rechaçariam em relacionamentos pessoais. A perda do senso de privacidade conduz a um fornecimento menos seletivo de dados pessoais e, com isso, a condutas imprudentes. A aceleração da informação, das relações comerciais e das interações intensifica a sensação de imediatismo iniciada desde a Primeira Revolução Industrial. Agora, contudo, a velocidade é muito superior, o que confere uma sensação de imediatismo, fugacidade e obtenção rápida daquilo almejado pelo usuário.

Assim, torna-se tarefa reducionista considerar, após a consumação de uma fraude ou invasão de dispositivo informático, que a vítima deveria ter previsto ou contemplado o aspecto ardiloso. Deve-se ponderar que há enorme leque de suscetibilidade dos indivíduos, de modo que poucos efetivamente não possuem fraquezas aptas a ser exploradas. Por essa razão, as circunstâncias concretas são essenciais.

Nesse esteio, Sydow aponta para a relevância do compartilhamento da responsabilidade por todos os agentes envolvidos, delineando-se o papel de cada qual (usuários, Estado, provedores de conexão, redes sociais) que agora integra inexoravelmente esse novo ambiente e, simultaneamente, perquirindo-se a "maturidade informática"[352] de cada usuário.

Essa análise casuística se faz necessária para efetiva observância ao valor constitucional do livre desenvolvimento da personalidade, que pressupõe condições efetivas de adoção de uma decisão racional pelo indivíduo como forma de efetiva promoção do bem jurídico individual tutelado, quer se trate da autodeterminação informática, quer se esteja diante do patrimônio.

Para tanto, considerando o plexo de tarefas desempenhadas pelos usuários virtualmente e os deveres de cautela delas decorrente, é consectário lógico o delineamento de certos perfis de vítimas mais suscetíveis a esses crimes, quer por objetivos próprios, quer por

---

[351] Ibidem, p. 40.

[352] Termo empregado por Sydow ao se referir ao consentimento do usuário quanto ao delito de invasão de dispositivo informático. (SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021, p. 694).

vulnerabilidades inerentes ao indivíduo.[353] As diretrizes desses perfis são traçadas pelas teorias criminológicas elencadas, que apontam aos principais fatores vitimais responsáveis pela criminalidade informática. A seu turno, não se abdica das tradicionais propostas classificativas vitimológicas (Capítulo 4.1.), que recebem devidas adaptações ao ambiente informático.[354]

Para efetuar uma tentativa de agrupamento em perfis de vítimas informáticas, com base na lição de Sydow, busca-se, a partir da classificação vitimológica tradicional, traçar perfis de indivíduos com tendência a se abster dos deveres de proteção elencados no Capítulo 4.3.2. (Atitudes preventivas da vítima nos crimes informáticos). Na distinção proposta por Sydow, trata-se de usuários em "exposição informática ativa", pouco preocupados com uma navegação segura, o que colabora para sua vitimização,[355] na linha dos estudos baseados na teoria geral do crime, na teoria das atividades rotineiras e na teoria da prevenção situacional do crime. Por outro lado, exclui-se a "exposição informática passiva", referente à adoção de todas as cautelas necessárias para o uso com segurança, na medida do exigível de cada usuário, minimizando-se os riscos a que todos naturalmente estão sujeitos.

Propõe-se a subdivisão dos agrupamentos, na linha da RAT, em três características principais: a) atividades online arriscadas (vítima solitária, gananciosa e curiosa e descuidada), b) ausência de guardião capaz (vítima ignorante); c) idade (idosos e jovens). Não se trata de perfis independentes e excludentes entre si, mas intercambiáveis e fluidos, de tal maneira que um mesmo usuário pode se enquadrar em diversos deles em suas atividades no ambiente virtual.

Deve-se pontuar ainda que, principalmente quanto à prática de atividades arriscadas no meio virtual, esse agrupamento também apresenta forte compatibilidade com uma menor capacidade de autocontrole das vítimas (movidas por desejos e ilusões que as tornam mais ingênuas e vulneráveis), a permitir notória correlação com a teoria geral do crime em seu viés vitimológico.

O primeiro perfil, conforme a classificação de Sydow, consiste na vítima solitária. É fato que os dispositivos informáticos são predominantemente individuais, contudo, podem ser

---

[353] Aliás, o legislador penal já reconhece situações de maior vulnerabilidade de determinadas vítimas, apenando com maior gravidade as condutas em face delas praticadas. Trata-se da previsão de circunstâncias agravantes do artigo 61, merecendo destaque o inciso "h": crianças, maiores de sessenta anos, enfermos ou mulheres grávidas.

[354] Nesse esteio, o escopo de determinar certos perfis de usuários não guarda qualquer relação com simples rotulamento, em espécie de *labelling approach* vitimal, mas, em verdade, mostra-se relevante para elencar vítimas que careçam de efetiva e especial tutela penal, dissociando-a de outras merecedoras de atenção por outros ramos jurídicos, tendo em vista um alinhamento político-criminal que confira primazia a uma prevenção de delitos mediante intervenção mínima do direito penal. No mais, sempre se mostra imprescindível análise casuística da conduta praticada, não somente em razão da heterogeneidade do perfil dos ofendidos, como também da multiplicidade de condutas potencialmente típicas praticadas no ambiente informático.

[355] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, p. 167.

utilizados pelos usuários como forma de suprir a carência de convívio em sociedade, potencializando seu interesse por materiais de cunho erótico (solidão antissocial), ou ainda, como busca por obter laços afetivos de amizade ou relacionamento (solidão relacional).

No primeiro caso, a antissociabilidade favorece a busca por materiais eróticos no ambiente virtual dentre usuários mais liberais. Assim, se tornam mais suscetíveis a ataques informáticos disfarçados de material erótico, posto que este consiste frequentemente em um chamariz para a instalação de *malwares.* No tocante à solidão relacional, os usuários buscam contato com pessoas desconhecidas por meios virtuais e redes de relacionamento, em razão da falta de companhia na realidade.[356]

Na sequência, Sydow apresenta a noção de vítima ignorante. Não se trata de ignorância das leis, mas efetivamente de não ter ciência dos riscos informáticos ou de manejo do ambiente virtual. A ignorância acerca da existência de riscos informáticos está praticamente erradicada na atualidade, em que há inesgotáveis informações acerca dos perigos e ameaças em rede.[357] Assim, salvo raras hipóteses de indivíduos recém-inseridos no ambiente, sem qualquer instrução prévia – como indígenas -, não se pode suscitar na sociedade atual referida ignorância.

A ameaça preponderante diz respeito, portanto, à ignorância tecnológica, ou seja, na falta de conhecimentos sobre os recursos informáticos. Nessa hipótese, não se exige que todo usuário obtenha expertise aprofundada a fim de evitar ataque complexo por um *cracker* mas, em verdade, uma conduta cautelosa na navegação em Internet, recorrendo ao auxílio por pessoas confiáveis em caso de dúvidas sobre como proceder.

A ignorância tecnológica se mostra uma das principais questões a se abordar para prevenção de novos crimes, considerando-se a heterogeneidade dos perfis de usuários, dotados de diferentes graus de conhecimento informático. Com efeito, a sociedade em rede inclui o mundo todo, mas não todo o mundo. Afinal, embora ela afete todas as pessoas, quer por sua lógica de funcionamento, quer por suas relações de poder, ainda existem indivíduos dela excluídos.[358] Nesse contexto, também as ciências criminais "devem adotar como ponto de partida esse novo paradigma de sociedade globalizada e excludente sempre que pretenderem

---

[356] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, pp. 171-172.
[357] Ibidem, pp. 172-173.
[358] CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006, p. 18.

Há uma divisão digital constatada por Castells nos Estados Unidos, marcada pelos possuidores e não possuidores de Internet. Embora haja paulatino aumento de acesso à rede informática pela sociedade, há também certa tendência de que reflita desigualdades sociais: proporcionalmente, naquele país, há menor acesso à Internet por grupos minoritários, como afroamericanos e hispânicos. (CASTELLS, Manuel. *The Internet Galaxy: reflections on the lnternet, business and society*. New York: Oxford University Press, 2001, pp. 247-248

ser efetivas em seus papéis de entendimento e equalização dos fenômenos criminais tais como têm se apresentado na atualidade".[359]

Por conseguinte, para uma abordagem jurídico-penal imediata da problemática da vítima ignorante, uma análise casuística, à luz das características pessoais do usuário, permite perquirir sobre seu grau de informação e de autodeterminação, a fim de não se impor um padrão de cautela inatingível para a maioria da população. Por essa razão, aliás, traça-se o panorama do *homem médio*, instituto que não se encontra alheio a dificuldades de delimitação em qualquer seara que se analise. Nesse ponto, à toda evidência, a cidadãos simples e que pouco possuam acesso à Internet torna-se defesa a imposição das cautelas ora propostas.

Ainda há grande dificuldade dos usuários em distinguir sites ilegítimos de *scamming*, o que reforça a necessidade de conscientização da população como principal mecanismo preventivo. Por essa razão, em razão do perfil médio da população, não se pode impor deveres de cautela sofisticados, mas apenas condutas mínimas, notadamente aquelas sintetizadas no Capítulo 4.3.2. (Atitudes preventivas da vítima nos crimes informáticos).

Convém ponderar, em adendo à classificação de Sydow, que parcela significativa das vítimas possui ciência das cautelas mínimas a se adotar quando de uma navegação virtual, de modo a não se enquadrar como vítima ignorante. Contemplam os delitos informáticos como uma ameaça distante, descartando sua suscetibilidade, posto que creem possuir conhecimentos necessários para evitar ataques por meio informático. Trata-se, com isso, da vítima descuidada, a qual naturalizou suas condutas cotidianas no ambiente digital em razão do uso cotidiano em normalidade e, portanto, não se mantém alerta para as ameaças em razão de negligência, deflagrada por excesso de confiança e de otimismo.

Na sequência, Sydow apresenta o perfil da vítima gananciosa: mais suscetível a práticas de engenharia social, culminando com o delito de estelionato, esse indivíduo busca obter vantagens, em regra financeiras, a partir de anúncios no ambiente informático. Trata-se de e-mails, sites e anúncios acerca de produtos em preço extremamente vantajoso, ou mesmo que fraudulentamente informam o recebimento de valores – como o golpe do bilhete premiado, ou recebimento de algum produto em sorteio, herança de parente distante.[360]

No mais, também é relevante a vítima curiosa, não dotada de ignorância tecnológica, porém em busca de informações sobre condutas ilícitas ou de cunho erótico, tabus.[361] A conduta

---

[359] SHECAIRA, Sergio Salomão. *Criminologia*. 6. ed. São Paulo: Revista dos Tribunais, 2014, p. 32.
[360] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, pp. 183-185.
[361] Ibidem, pp. 186-187.

pode estar associada à solidão antissocial, atrelada à pornografia, mas a ela não se resume: inclui a busca por conhecimento sobre produtos ilícitos, como jogos de azar, comércio de armas, além de imagens de acidentes, atentados. A tentativa de acesso à *darkweb*, por curiosidade, pode culminar com grande exposição a vulnerabilidade para um usuário de conhecimento informático mediano. Nessas hipóteses, é imprescindível conhecimento técnico, inclusive para evitar ataques informáticos ou crimes mais graves, visto que nela se concentram diversas organizações criminosas.

Por fim, merecem destaque as vítimas de crimes informáticos em razão de sua vulnerabilidade presumida: idosos e jovens (crianças/adolescentes). Aqueles se inserem em uma sistemática jurídica especial de proteção, capitaneada pelo artigo 230 da Constituição Federal, bem como pela sistemática do Estatuto do Idoso. Pessoas de idade avançada apresentam maiores dificuldades visuais, que podem ser exploradas no ambiente informático. Ademais, muitos idosos possuem rotina solitária nessa fase da vida, sendo potenciais vítimas sob a ótica da solidão relacional. Por fim, e principalmente, muitos idosos apresentam especial fragilidade informática, posto que já apresentavam idade avançada quando do surgimento de novas tecnologias, apresentando domínio limitado. Portanto, também apresentam ignorância tecnológica, porém, em razão de falta de capacidade ou habilidade de aprendizado. [362] Assim, apesar de pesquisas demonstrarem maior incidência de crimes informáticos em face da população jovem, não há dúvidas acerca da especial vulnerabilidade dos idosos, notadamente no tocante a crimes informáticos impróprios, como estelionato mediante *phishing*.

Vítimas jovens, do mesmo modo, estão sujeitas a especial atenção estatal por meio do Estatuto da Criança e do Adolescente, em razão de sua fragilidade. No ambiente virtual, crianças (até 12 anos incompletos) devem efetuar navegação sempre acompanhada de um responsável, bem como estabelecendo-se filtros de conteúdo. Sua imaturidade favorece a prática de crimes informáticos ora tratados e, com frequência, crimes de maior gravidade, como contra a dignidade sexual.

Adolescentes, por outro lado, paulatinamente conquistam maior autonomia no ambiente virtual, o que, contudo, pode torná-los suscetíveis a ataques virtuais. À medida que adquirem certo conhecimento tecnológico, também maximiza sua curiosidade no ambiente virtual. Esses fatores, aliados a certo grau de imaturidade e ingenuidade, levam-nos a grande exposição a crimes informáticos. Assim, é necessário acompanhamento de responsáveis, ainda que mais flexível – em observância ao respeito a sua identidade e autonomia, nos termos do

[362] SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática*. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009, pp. 176-177.

artigo 17, do Estatuto da Criança e do Adolescente –, e sempre com filtro de conteúdo, bem como limitando seu acesso a redes sociais e salas de bate-papo conforme a classificação indicativa recomendada.

Fixadas as balizas criminológicas e vitimológicas para os crimes informáticos, extrai-se seu substrato empírico para confluência e aproveitamento pela dogmática penal. E sua manifestação pode ser subsividida em duas vertentes paralelas, porém não excludentes. Por um lado, no próximo Capítulo buscar-se-á compreender a influência que a vitimodogmática deve desempenhar sobre os crimes informáticos e em que medida o princípio da autorresponsabilidade deve influenciar a responsabilidade penal nos casos concretos, levando-se em consideração a complexidade da vítima no ambiente virtual.

Ademais, no último Capítulo será promovida análise do funcionalismo penal nos delitos informáticos, com enfoque sobre sua vertente moderada, que propugna justamente a imprescindibilidade de aportes político-criminais para a delimitação da responsabilidade penal.

Desde logo, é possível constatar que idosos e jovens, grupos especialmente tutelados de forma pelo ordenamento jurídico e no Código Penal, em regra não podem estar sujeitos aos princípios vitimodogmáticos ou propostas funcionalistas de mitigação ou exclusão da responsabilidade do agente, dada sua vulnerabilidade inerente e potencialização do efeito desinibidor virtual. Uma análise casuística, por outro lado, poderá apontar conhecimento informático-tecnológico elevado inclusive nesses grupos, o que ensejaria nova incidência do princípio da autorresponsabilidade.

No mais, o perfil dos demais grupos de vítimas, intrinsecamente relacionado a atividades online arriscadas (como a vítima solitária, gananciosa, curiosa) e ausência de guardião capaz (vítima descuidada e ignorante), potencializado por reduzido autocontrole dos usuários, pressupõe análise concreta para se aferir quais cautelas foram adotadas e, em caso de negligência, viabilizar eventual atenuação da responsabilidade penal do agente, que sob a ótica vitimodogmática, quer sob o funcionalismo moderado.

5. VITIMODOGMÁTICA E CRIMES INFORMÁTICOS

Neste Capítulo busca-se a conjugação dogmático-penal entre os fundamentos constitucionais da tutela aos crimes informáticos e a base empírica fornecida pela criminologia.

A vitimodogmática emerge historicamente como um mecanismo de recuperação da dignidade da vítima na dogmática penal, realçando-a como ser racional e autônomo. A noção de autorresponsabilidade, lastro dos desenvolvimentos vitimodogmáticos, estabelece um âmbito de organização prioritário à vítima, a quem incumbe sua destinação conforme o livre desenvolvimento de sua personalidade, em oposição ao denominado paternalismo penal.

No ambiente virtual, como se verá, a autorresponsabilidade implica a admissão de que o usuário assume riscos, ainda que redundem em lesão sob o aspecto naturalístico, em que se verifica, na verdade, efetivo exercício do bem jurídico individual tutelado – a autodeterminação informática ou o patrimônio.

Assim, a compreensão das correntes vitimodogmáticas traz uma relevante discussão acerca do papel do usuário na prática e prevenção de crimes informáticos, refletindo-se quais seus reflexos sobre a responsabilização penal do agente à luz dos estudos vitimológicos e dos perfis de vítimas. Dessa forma, sobressai a relevância das teorias criminológicas emergentes na seara informática, notadamente a teoria geral do crime, a teoria das atividades rotineiras e a prevenção situacional do crime, lastro empírico que converge com a tutela constitucional da autorresponsabilidade.

Esse raciocínio é dotado de grande relevância nos crimes informáticos ora analisados, em que houve recente recrudescimento das penas, verificando-se sanções exacerbadas nos delitos de fraude informática e furto qualificado mediante fraude por invasão de dispositivo informático ou eletrônico, em violação aos princípios da intervenção mínima e culpabilidade.

5.1. A relevância da vitimodogmática no Direito Penal

Como aponta Frommel, o ramo criminal em que os atos e interesses da vítima mais foram relegados não consistiu no processual ou na reparação do dano, mas efetivamente na dogmática penal.[363] Principalmente em razão do causalismo, mas também em certa medida com

[363] FROMMEL, Monika. Opferschutz durch hohe Strafdrohungen: Der vergiftete Apfel vom Baume des Punitivismus. *Monatsschrift für Kriminologie und Strafrechtsreform*, v. 68, p. 350-359, 1985, p. 350 *apud* SILVA SÁNCHEZ, Jesús María. Innovaciones teórico-prácticas de la Victimología en el Derecho penal. In: *Victimología: VIII Cursos de Verano en San Sebastián = VIII Udako Ikastaroak Donostian.* Universidad del País Vasco/Euskal Herriko Unibertsitatea, pp. 75-83, 1990, p. 79.

o finalismo, o delito é contemplado de forma unilateral, entendido como uma causação de lesão a um bem jurídico ou violação à norma penal. É bem verdade que certos delitos em espécie, como estupro e estelionato, conferiam relevância ao comportamento do sujeito passivo. Ocorre que ainda assim a vítima segue fora do papel protagonista do fato criminal. [364]

Contudo, no entendimento de Beristain, a vitimologia "pode e deve enriquecer, radicalmente, a teoria e a práxis do nosso controle social e, em especial, do Poder Judiciário (penal)."[365] Afinal, propugna uma nova abordagem da vítima, levando a uma desjuridicização do controle social penal, notadamente no que tange à prevenção à vitimação, bem como a uma assistência à vítima do delito, prevenindo-se, quando da ocorrência delitiva, as vitimizações secundária e terciária.[366]

O reconhecimento dessa inter-relação entre autor e vítima, vítima e vitimário, apenas contribui para a consolidação das ciências penais, inclusive no âmbito dogmático. Como aponta Beristain:

> Ainda hoje muitos e eminentes penalistas opinam que o Código Penal é o código dos delinquentes, mas não o código das vítimas. Outros, ao contrário, opinam que já não cabe manter vigente um Código Penal que se apóia na dogmática pela qual se possam entender e compreender a sanção e o delinqüente sem uma constante e radical referência às vítimas. Estas são a outra face da única moeda que atualmente tem curso legal. Basta ler um livro de vitimologia para ver que o delinquente está, inseparável e consubstancialmente, relacionado com a vítima, mais que o corpo com sua sombra. [367]

Para Silva Sánchez, uma efetiva pacificação do conflito entre autor e vítima, sendo desta o interesse primário, apenas pode ser efetivada mediante uma distinção entre a responsabilidade pelo fato correspondente a cada parte. Apenas por essa via é possível que o Direito Penal efetivamente cumpra sua função social de prevenção de delitos dentro do marco de observância aos princípios da intervenção mínima e da culpabilidade. Com efeito, estratégias punitivistas não favorecem as vítimas, mas, em verdade, exercem função meramente simbólica face à opinião pública, sem uma efetiva proteção do ofendido.[368]

---

[364] SILVA SÁNCHEZ, Jesús María. Innovaciones teórico-prácticas de la Victimología en el Derecho penal. In: *Victimología: VIII Cursos de Verano en San Sebastián = VIII Udako Ikastaroak Donostian*. Universidad del País Vasco/Euskal Herriko Unibertsitatea, pp. 75-83, 1990, p. 80.

[365] BERISTAIN, Antonio. *Nova criminologia à luz do direito penal e da vitimologia*. Brasília: Editora Universidade de Brasília, 2000, p. 123.

[366] Nesse contexto, a abordagem vitimológica confere enfoque na prevenção delitiva. Em caso de vitimação, visa a conceber um método restaurativo – capitaneado pela justiça restaurativa –, superando-se o paradigma retributivo, de modo a se coadunar como melhor abordagem à proteção dos indivíduos vitimados. (BERISTAIN, Antonio. *Op. cit.*, p. 124).

[367] BERISTAIN, Antonio. *Op. cit.*, p. 191.

[368] SILVA SÁNCHEZ, Jesús María. La víctima en el futuro de la dogmática. *Victimología*. San Sebastián: Universidad del País Vasco/Euskal Herriko Unibertsitatea, 1990, p. 233.

Neste ponto, surge a relevância da vitimodogmática: trata-se de uma aplicação dos postulados vitimológicos sobre o direito penal, a fim de se perquirir sobre a contribuição da vítima para a configuração de uma conduta delitiva, em todos seus elementos analíticos (fato típico, antijurídico e culpável), na parte geral e especial do Código Penal, bem como na repercussão sobre a aplicação da pena.[369]

Nesse sentido também sustenta Meliá, ao apontar como ponto fulcral da vitimodogmática a análise sobre eventual repercussão da "corresponsabilidade da vítima" sobre a valoração jurídico-penal do fato praticado pelo autor.[370]

Como aponta Greco: "ela surgiu da necessidade de se abandonar uma visão simplista do fenômeno criminoso, em que de um dos lados teríamos uma pessoa totalmente inocente (vítima), e de outro, uma pessoa totalmente culpada (criminoso),"[371]

Indubitavelmente, parcela significativa dos argumentos elencados a favor de teoria vitimodogmáticas apresenta viés político-criminal. Um dos aspectos centrais consiste em propor medidas de autoproteção às vítimas a fim de evitar sua futura "vitimização". Isso porque o excesso de confiança derivado da imposição de uma pena àquele delito conduz o titular do bem jurídico a atitudes mais displicentes. Ao se suprimir essa confiança, com a determinação de medidas preventivas à vítima, haveria um declínio de criminalidade.[372_373]

O desenvolvimento da vitimodogmática, em compasso com a vitimologia, apenas adquiriu maior relevância na segunda metade do século XX. Isso ocorreu por meio de estudos centrados no âmbito patrimonial, notadamente nos delitos de revelação de segredos privados, estelionato e apropriação indébita. A investigação acerca do erro ou engano no delito de

---

[369] Nesse contexto também se deve ressaltar a importância desempenhada pelas teorias funcionalistas, por meio da teoria da imputação objetiva, que permite um resgate do enfoque sobre a vítima ao buscar delinear o papel por ela desempenhado na criação e manifestação do risco produzido, o que será analisado em Capítulo próprio.

[370] A vitimodogmática rechaça as críticas de que uma atribuição à vítima da responsabilidade pelo resultado culminaria com uma vitimização secundária por meio de sua instrumentalização para fins político-criminais. Isso porque, ao se desconsiderar uma intervenção relevante da vítima para o acontecer típico, automaticamente haveria uma sobrerresponsabilização do autor, em violação ao princípio da culpabilidade. Ou seja, em verdade haveria uma excessiva culpabilização do autor, em espécie de "blaming the comitter." Logo, toda opção de direito penal mínimo e liberal deve levar a sério a vitimodogmática, para traçar limites à responsabilidade do autor proporcionalmente àquilo que realizou. (SILVA SÁNCHEZ, Jesús María. La víctima en el futuro de la dogmática. *Victimología*. San Sebastián: Universidad del País Vasco/Euskal Herriko Unibertsitatea, 1990, p. 234-235).

[371] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 39.

[372] ROXIN, Claus. *Politica Criminal y estrutura del delito.* Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992, p. 69.

[373] Meliá também sinaliza para uma tentativa de distanciamento das concepções clássicas da política de *Law and Order*, marcada por penas elevadas e seletividade na persecução penal, o que, na realidade, conduz a uma efetiva desproteção da vítima. (MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, pp. 361-362.

estelionato recebeu diversos aportes com base no comportamento da vítima, como em hipóteses de dúvida e torpeza bilateral.

Nesse contexto, tem recebido significativa adesão a categorização proposta por Schultz entre delitos de relação e delitos de intervenção. Para o autor, aqueles são "fatos gerados em uma determinada relação humana ou ao menos determinados de modo decisivo por tal relação".[374] Um delito de relação pressupõe um confronto direto e atual entre autor e vítima, sendo exemplo emblemático o estelionato. A seu turno, em regra, o furto não se enquadra nessa categoria, salvo em hipóteses de fraude. Os delitos de intervenção, por outro lado, não pressupõem participação da vítima na conduta, posto que o autor é quem unicamente intervém no bem jurídico independentemente de seu titular.[375]

Essa classificação foi incorporada por R. Hassemer em seu arcabouço vitimodogmático, sustentando o autor que, em delitos de relação, caso a vítima deixe de adotar medidas mínimas de autoproteção, dispensa-se a tutela penal, enquanto em delitos de intervenção remanesce a proteção pelo ordenamento, que poderá sofrer mitigações.[376]

Paulatinamente, a lente vitimodogmática começa a transcender sua aplicação, antes limitadas a hipóteses específicas em alguns delitos patrimoniais. Há uma tendência a se tornar uma teoria dogmática que traz aportes concretos à teoria do delito e aos tipos penais (relacionais, ao menos) em espécie. Sua influência passa a ser notória em hipóteses de consentimento do ofendido, ou mesmo na seara da teoria da imputação objetiva,[377] com contribuições acerca dos conceitos de incremento de risco (se o risco produzido pelo autor seria apto para produção do resultado), autocolocação em perigo e heterocolocação consentida pela vítima.[378] Não se limita, contudo, a propostas funcionalistas, recebendo amplo campo de aplicação dentro da teoria finalista. Quanto aos delitos em espécie, sua influência supera os

---

[374] SCHULTZ, Hans. *Kriminologische und strafrechtliche Bermekungen zur Beziehung zwischen Täter und Opfer*. ZStrR, v. 71, p. 171-192, 1956, p. 172 *apud* MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 376.

[375] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 376.

[376] HASSEMER, Raimund. *Schutzbedürftigkeit des Opfers und Strafrechtsdogmatik. Zugleich ein Beitrag zur Auslegung des irrtumsmerkmals in § 263 StGB.* Berlin: Duncker & Hublot, 1981, pp. 52-55 *apud* MELIÁ, Manuel Cancio. *Op. cit.*, p. 377.

[377] Subjaz na concepção vitimodogmática o princípio da autorresponsabilidade, de modo que cada indivíduo, autônomo, responderá por seus próprios atos, inclusive riscos a seus bens jurídicos, como correlato do livre desenvolvimento de sua personalidade. Assim, para Zaczyk, Schünemann, Frisch, o princípio da autorresponsabilidade é apto a excluir o injusto. Contudo, critério marcante e diferenciador da vitimodogmática em relação à teoria da imputação objetiva consiste na ausência de uma normatização específica, sem uma inserção em um *topos* de análise da conduta típica. Para defensores da vitimodogmática, essa análise deve ser feita casuisticamente, à luz da parte especial (delitos em espécie) e do caso concreto. Outros autores, como Jakobs e Meliá, postulam a exclusão da imputação objetiva.

[378] SILVA SÁNCHEZ, Jesús María. La víctima en el futuro de la dogmática. *Victimología*. San Sebastián: Universidad del País Vasco/Euskal Herriko Unibertsitatea, 1990, p. 234.

crimes patrimoniais, atingindo crimes contra a dignidade sexual e delitos praticados por funcionários públicos.[379]

Frise-se que o cerne dos estudos vitimodogmáticos se afasta de condutas permeadas pela aquiescência do titular do bem jurídico (mediante acordo ou consentimento), para conferir o enfoque sobre condutas em que houve desídia de seu titular, que culposamente – ao não adotar medidas preventivas razoavelmente exigíveis – contribuiu com o resultado lesivo.

A vitimodogmática se torna, assim, um mecanismo de consolidação dogmático-penal do valor constitucional do livre desenvolvimento do indivíduo, reconhecendo-se o caráter autônomo da vítima, a quem incumbe o âmbito preferencial de organização de certos valores – sempre individuais e disponíveis. E esse protagonismo do indivíduo se coaduna com a teoria constitucional do bem jurídico-penal, que ressalta o caráter instrumental de sua tutela em favor do desenvolvimento da personalidade. Assim, a assunção de riscos materializada por uma conduta desidiosa pode implicar efetiva ou parcial realização do próprio bem jurídico, e não sua completa afetação sob a ótica penal.

Nesse contexto, a vitimodogmática torna-se uma ferramenta útil e necessária para a compreensão da dogmática que permeia os crimes informáticos próprios e impróprios patrimoniais, em sua maioria marcados por um envolvimento direto do próprio usuário (delitos de relação), que se torna uma vítima em potencial pelo simples fato de navegar em rede, mas principalmente quando promove uma exposição informática ativa. Com efeito, conforme delineado no Capítulo 4.3. (Novas propostas criminológicas aos crimes informáticos), sobretudo a teoria das atividades rotineiras e a teoria da prevenção situacional do crime revelam que a postura adotada pelo usuário no ambiente virtual traz influências condicionantes para as práticas de delitos informáticos objeto desta pesquisa, que podem ser classificados como delitos de relação (segundo a acepção de Schultz).

5.2. Principais correntes vitimodogmáticas

Com a expansão vitimodogmática em sede de delitos dolosos, principalmente delitos de relação, Silva Sánchez aponta para o desenvolvimento de duas posições divergentes na doutrina:[380] a) por um lado, a corrente majoritária e moderada, fortemente influenciada por

[379] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 378.

[380] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 163-194, 2001.

Winfried Hassemer, para a qual o comportamento da vítima deve ser ponderado quando da dosimetria da pena, não sendo apto a excluir a responsabilidade penal, salvo expressa disposição legal; b) d'outra sorte, Bernd Schünemann capitaneia a corrente minoritária, segundo a qual o princípio da autorresponsabilidade, que culmina com a *ultima ratio* penal, é apto a conduzir a uma isenção de responsabilidade (pela via da tipicidade) quando a vítima possui dever de proteção de sua esfera a partir de atitudes razoáveis e usuais exigíveis em sociedade. Por fim, procede-se a uma síntese dessas correntes, recorrendo-se aos entendimentos e críticas esposados por Cáncio Meliá e Silva Sánchez.

Com isso, busca-se promover uma subsunção dessas correntes à análise dos crimes informáticos próprios e patrimoniais impróprios, tendo por amparo teórico a fundamentação constitucional da teoria do bem jurídico, além do respaldo empírico das teorias criminológicas apreciadas no Capítulo 3.

5.2.1. Corrente majoritária

Uma posição moderada é adotada por autores como Rudolph Hassemer, Hillemkamp e Arzt, que concebe influência relevante da conduta da vítima apenas quando da fixação da pena. Há um reconhecimento de que a imposição da atipicidade em hipóteses de possibilidade de atuação da vítima levaria a uma inversão de papéis com o autor, a exacerbar culpabilização da vítima e desconfiança social. Por outro lado, esses autores sustentam que desconsiderar completamente a vítima implicaria uma sobrecarga penal sobre o autor, ao qual a conduta não é exclusivamente imputável, lesionando os princípios da culpabilidade, proporcionalidade e fragmetariedade. Assim, a adoção de posturas radicais, em ambos os sentidos, implicaria soluções inadequadas: eis o dilema vitimológico.[381]

Diante dessa ambiguidade, é recomendável a adoção de uma postura matizada, que passa pela distinção entre delitos dolosos e culposos. Nesta hipótese, concorrendo atuação imprudente da vítima, haveria uma violação ao dever de cuidado pelo autor, o que seria apto a excluir a própria imputação em certas hipóteses. Trata-se de casos especialmente delineados pela teoria da imputação objetiva no tocante à autocolocação da vítima em risco e à heterocolocação em risco consentida, como se verá mais detidamente no Capítulo 6.5. (Propostas para a autocolocação em risco nos crimes informáticos).

---

[381] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 163-194, 2001, p. 170.

Paulatinamente, o postulado de valoração de conduta da vítima atinge delitos comissivos dolosos, porém inserido no âmbito de dosimetria da pena, com atenuação da responsabilidade do autor tendo em vista a redução da danosidade social (princípio da ofensividade) e menor culpabilidade do autor.[382]

Para Hillenkamp, a atenuação da pena do autor consiste na única aplicação admissível da vitimodogmática, posto que uma consideração no âmbito da tipicidade, com total exclusão da tutela penal, privaria a vítima de tutela e impor-lhe-ia deveres irrazoáveis em sociedade, fatores que não são dogmaticamente sustentáveis. Ademais, aponta o autor que, ao se excluir, sem qualquer amparo legal, condutas que gramatical e semanticamente se amoldam ao tipo penal haveria flagrante violação ao princípio da legalidade.[383]

Apesar de apresentar adesão majoritária da doutrina, inclusive no Brasil, a corrente majoritária, ao nosso sentir, peca por excessiva timidez. Em terras pátrias, limita-se a uma dentre as diversas circunstâncias judiciais previstas no artigo 59, do Código Penal, quando da fixação da pena-base. Se não bastasse, a necessidade de observância à pena mínima prevista para o tipo penal frequentemente culmina com sua total inaplicabilidade e, como decorrência lógica, violação ao princípio da culpabilidade – posto que inócua a postura da vítima na fixação da pena.

Essas limitações são sobremaneira evidenciadas nos delitos informáticos próprios (face ao bem jurídico autodeterminação informática) e impróprios (face ao patrimônio), dado o papel central do usuário na gênese delitiva, como comprovado pelas principais teorias criminológicas emergentes. Uma aplicação pura e simples da corrente majoritária implica uma excessiva simplificação do instituto vitimodogmático dentro da atual sociedade de risco e em rede. Notadamente a teoria das atividades rotineiras e prevenção situacional do crime delineiam a complexidade de fatores relevantes para a prevenção delitiva, nele incluídas condutas minimamente esperadas dos usuários como titulares dos dispositivos integrados no ambiente virtual.

E esse papel protagonista, sob o viés criminológico, implica conferir maior relevância aos usuários também na seara penal, de maneira que deve ser ponderado na própria conformação do tipo penal, além de ensejar maior sopesamento quando da dosimetria da pena

---

[382] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 163-194, 2001, p. 172.
[383] Ibidem, p. 157.

– quer em prol de seu incremento, quer em prol de redução mais significativa do que aquela promovida pelo artigo 59, na atual redação do Código Penal.

5.2.2. Corrente minoritária

Parte minoritária da doutrina, capitaneada por Bernd Schünemann, mune-se da vitimodogmática como forma de isenção da responsabilidade do agente, excluindo-se até mesmo a tipicidade do delito diante de conduta desidiosa da vítima que contribuiu para o resultado. Ou seja: ainda que inexistente anuência expressa ou tácita da vítima (mediante acordo ou consentimento), seu grau excessivamente culposo de atuação levaria a uma irresponsabilidade penal do autor.

Para essa corrente, relegar a vitimodogmatica ao âmbito da dosimetria penal culminaria com uma inoperância concreta de seus institutos.[384]

Adepta a um direito penal de intervenção mínima (ou *ultima ratio*), essa corrente recorre aos princípios penais voltados à restrição do *ius puniendi*, notadamente fragmentariedade e subsidiariedade. A partir de um raciocínio dedutivo, Schünemann postula a atipicidade de condutas diretamente causadas ou facilmente evitáveis pela vítima, posto que a esfera penal não seria o único e tampouco último mecanismo de proteção do bem jurídico. Isso porque o princípio da subsidiariedade não está restrito apenas a outros mecanismos estatais de proteção, mas a qualquer forma eficaz de controle social, nela incluída a autoproteção razoável e usual do sujeito passivo. [385]

Em relação intrínseca com a *ultima ratio*, Schünemann aplica o princípio vitimológico como uma regra de interpretação sistemática dos tipos penais, mitigando-se ou inclusive afastando-se responsabilidade para hipóteses em que a vítima não merece nem necessita de proteção penal: vale dizer, caso a lesão ao bem jurídico pudesse ser evitada por uma conduta inserida no âmbito de proteção incumbido ao sujeito passivo. O princípio vitimológico pode ser sintetizado, assim, pela noção de autorresponsabilidade (Selbstverantwortungsprinzip).

Para Schünemann, o princípio vitimológico obtém guarida na parte geral como critério interpretativo das categorias de imputação por consistir em um mecanismo hábil a refrear a

---

[384] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 173.

[385] Do mesmo modo, considerando-se a postura adotada pela vítima, não se verifica grave desvalor social da conduta praticada pelo agente, de modo a obstar a incidência penal, limitada pelo princípio da fragmentariedade apenas às violações de maior magnitude.

criação de categorias supralegais em desfavor do réu. Mas não é só. Deve incidir sobre os tipos da parte especial, sendo fator essencial para a compreensão do bem jurídico tutelado.[386][387]

Para Schünemann, ao se vislumbrar a interpretação da parte especial sob a ótica da *ultima ratio*, impõe-se uma restrição à discricionariedade do legislador.[388] Nessa hipótese, segundo o autor, a limitação ao direito penal fomenta a proteção dos bens jurídicos, porquanto transmite a mensagem de que o dano social, causado por um comportamento da vítima em renúncia a seus próprios interesses, é apto a induzir condutas de autoproteção do sujeito passivo. Com esse raciocínio, demonstra-se o interesse na tutela penal apenas de pessoas efetivamente carecedoras e merecedoras de proteção.

No mesmo sentido, Raimund Hassemer preconiza que, apesar de o tipo penal desvelar um risco *ex ante* ao bem jurídico tutelado, sua concreção ou efetiva lesão deve ser verificada *ex post*. Dessa maneira, caso haja contribuição decisiva da vítima para a prática delitiva, deve-se perquirir se ela exerceu as faculdades exigíveis de autodefesa. Em caso negativo, ela se torna corresponsável pela lesão ao bem jurídico. Como aponta Greco, não se trata de co-culpabilização da vítima, mas sim de efetiva imputação ao agente, na medida de sua culpabilidade, conforme preconiza a lição penal. Assim, a depender do grau de contribuição da vítima, torna-se viável uma redução da pena, ou mesmo atipicidade da conduta.[389]

Para uma correta aplicação do princípio da autorresponsabilidade, conforme expõe Raimund Hassemer, o titular do bem jurídico deve possuir a faculdade e capacidade de evitar ataques ao bem jurídico, o que o autor sintetiza como possibilidade de autotutela (S*elbstschutzbedürftigkeit*). Desse modo, não se exige autoproteção por pessoas com

---

[386] Exemplificativamente, entende o autor pela ausência do delito de falsificação de moeda diante de sua inaptidão a enganar o homem médio, posto que grosseira, o que tampouco configuraria estelionato. SCHÜNEMANN, Bernd. El sistema del ilícito jurídico-penal: concepto de bien jurídico y victimodogmática como enlace entre el sistema de la parte general y de la parte especial. In: HERNÁNDEZ, Moisés Moreno (Coord.). *Problemas capitales del moderno derecho penal a principios del siglo XXI*, Editorial Ius Poenale, México D.F., pp. 87-113, 2003, p. 122.

[387] Esse critério interpretativo ocorre em observância ao princípio da legalidade, tendo em vista que se atém ao núcleo conceitual (*Begriffskern*), de modo a respeitar o âmbito gramatical contido no tipo penal. A influência ocorre apenas sobre o campo conceitual (*Begriffshof*), cujo alcance, embora limitado gramaticalmente, pode ser moldado conforme a subsidiariedade e o princípio vitimológico, tornando-se verdadeira interpretação teleológica restritiva do tipo penal. (SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 176).

[388] SCHÜNEMANN, Bernd. O direito penal é a ultima ratio da proteção de bens jurídicos: sobre os limites invioláveis do direito penal em um estado de direito liberal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 13, n. 53, p. 9-37, mar./abr. 2005, pp. 34-35. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=50732. Acesso em: 5 out. 2020.

[389] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 43.

capacidade restrita de decisão (como jovens e enfermos mentais), ou mesmo esforço hercúleo para obstar o resultado lesivo.[390]

O raciocínio da corrente minoritária reverbera sobre os delitos informáticos na seguinte medida: usuários que apresentem perfis de vítimas descuidadas, ignorantes ou mesmo solitárias, em regra, serão desmerecedores de proteção penal diante de prática ou navegação digital negligente ou imprudente. Isso porque o próprio titular do bem jurídico (quer se esteja diante da autodeterminação informática (nos crimes próprios), quer do patrimônio (nos crimes impróprios, dentro do recorte proposto) não exerceu seus deveres mínimos de cautela no ambiente virtual, notadamente aqueles constatados por meio da teoria das atividades rotineiras.[391] Ainda, incidência do princípio da subsidiariedade se manifesta diante das diversas alternativas de prevenção delitiva, mormente aquelas condutas minimamente esperadas do usuário médio no ambiente virtual.

Por outro lado, o raciocínio esposado ainda assim não incidiria sobre vítimas idosas, jovens ou ignorantes, porquanto sobre elas não recai o princípio vitimológico em sua plenitude. Tampouco se poderia falar de aplicação da subsidiariedade penal posto que, normalmente, trata-se de perfil de vítimas desprovidas de capacidade plena de autoproteção, carecendo em maior medida de tutela penal.

5.2.2.1. Aspecto jusfilosófico da vitimodogmática para a corrente minoritária

Schünemann, Fiedler e Zaczyk constroem a esfera de proteção da vítima sob o conceito de autorresponsabilidade, lastreados em conceito de autonomia e liberdade. Isso remonta a uma noção Kantiana de autodeterminação, ou seja, sua representação racional para atuação.

Conforme propõe Schünemann, a noção de *ultima ratio* no Direito Penal deriva da autorresponsabilidade, a qual, por sua vez, encontra suas raízes no contrato social: apenas nos aspectos em que os indivíduos não conseguiriam se proteger delegou-se a autonomia ao Estado, o qual seria hábil a desempenhar esse papel para além de capacidades individuais.[392] Logo, os cidadãos renunciam a tanta liberdade quanto indispensável para a proteção mútua das liberdades

---

[390] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 44.
[391] Cf. Capítulo 4.3. Novas propostas criminológicas aos crimes informáticos.
[392] GRECO, Luís. Comentário ao estudo de Schünemann "o direito penal é a ultima ratio da proteção de bens jurídico: sobre os limites invioláveis do direito penal em um estado de direito liberal". *In:* IBCCRIM. INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS *et al*. *IBCCRIM 25 anos*. Belo Horizonte: D'Plácido, 2017, p. 209.

individuais, de modo que o Estado concentra apenas tarefas que os indivíduos da sociedade, por si sós, não são aptos a desempenhar.[393]

O injusto penal consiste em uma violação à liberdade de outrem. Assim, quanto maior o domínio do resultado da conduta pela vítima, mais se afasta o comportamento do agente como constitutivo do injusto, o que implica reconhecer a inaptidão de uma autolesão ou de uma autocolocação consciente em risco para violar a norma penal.[394]

O princípio vitimodogmático deriva, portanto, da autonomia dos cidadãos, evitando-se sua instrumentalização ou paternalismo em um Estado Democrático de Direito,[395] no qual são vedadas imposições de concepções morais, religiosas, ou de determinadas formas de vida.

Deve-se considerar que o respeito à autonomia humana viabiliza uma inversão dialética, de modo a permitir uma proteção de debilidades do sujeito passivo em face de condutas abusivas de terceiros. Por essa razão, é viável o paternalismo indireto em casos de déficit de autonomia do indivíduo (por exemplo coação, erro, entre outros) ou mesmo para proteção de vulneráveis (como adolescentes e idosos).[396]

Ainda que se oponha a essa corrente, há notória relevância de seus fundamentos jusfilosóficos, que encontram eco na Constituição Federal por meio da dignidade da pessoa humana e do princípio do livre desenvolvimento do indivíduo. Como visto no Capítulo 1.1. (Desenvolvimento de um novo direito fundamental e sua construção constitucional), trata-se justamente dos aspectos basilares que inauguram novos direitos da personalidade na seara informática e, como decorrência, viabilizam a construção constitucional do bem jurídico autodeterminação informática.

---

[393] SCHÜNEMANN, Bernd. El sistema del ilícito jurídico-penal: concepto de bien jurídico y victimodogmática como enlace entre el sistema de la parte general y de la parte especial. In: HERNÁNDEZ, Moisés Moreno (Coord.). *Problemas capitales del moderno derecho penal a principios del siglo XXI*, Editorial Ius Poenale, México D.F., pp. 87-113, 2003, p. 112.
Schünemann resgata essa noção em Beccaria, para quem: "É seguro que cada um só quer entregar ao depósito público uma parte mínima de sua liberdade – apenas o suficiente para levar os outros também a protegê-lo. A soma dessas partes mínimas constitui o direito de punir; tudo o que a ultrapassar é abuso, e não justiça." (BECCARIA, Cesare. Dos *delitos e das penas*. Trad. Luciana Guidicini e Alessandro Contessa. São Paulo: Martins Fontes, 2005, p. 43).

[394] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 430.

[395] GRECO, Luís. Comentário ao estudo de Schünemann "o direito penal é a ultima ratio da proteção de bens jurídico: sobre os limites invioláveis do direito penal em um estado de direito liberal", (SCHÜNEMANN, Bernd. O direito penal é a ultima ratio da proteção de bens jurídicos: sobre os limites invioláveis do direito penal em um estado de direito liberal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 13, n. 53, p. 9-37, mar./abr. 2005. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=50732. Acesso em: 5 out. 2020).

[396] SCHÜNEMANN, Bernd. Die kritik am strafrechtlichen paternalismus - eine sisyphus-arbeit?. *In: PATERNALISMUS im Strafrecht*: Die Kriminalisierung von selbstschädigendem Verhalten. Organização de Ulfrid NEUMANN, Kurt SEELMANN. Baden-Baden: Nomos, p. 221-240, 2010. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=83488. Acesso em: 5 out. 2020.

Deve-se ponderar, ainda, a abrangência desse raciocínio sobre crimes informáticos patrimoniais impróprios, tendo em vista que toda a construção vitimodogmática tem sua origem justamente em reflexões acerca de delitos patrimoniais, considerando-se tratar de bem jurídico disponível por excelência.

Por essa razão, embora o ambiente virtual pressuponha certa regulamentação, é vedado tolher sobremaneira a liberdade de atuação dos usuários, sob pena de se incorrer em um paternalismo penal violador do próprio valor jurídico tutelado: nos crimes próprios, a integridade, disponibilidade e confidencialidade dos dados e informações; nos crimes impróprios ora estudados, o patrimônio. De fato, quanto maiores as limitações virtuais em prol da segurança dos usuários, menor será seu espaço de atuação e liberdades, pulverizando-se vigilância da navegação e dos conteúdos informáticos.

5.2.2.2. Críticas à corrente minoritária

A aplicação da vitimodogmática proposta pela corrente minoritária é alvo de inúmeras críticas. Um dos ataques mais veementes à corrente consiste na utilização inadequada do princípio da *ultima ratio*. Segundo Roxin, sob o ponto de vista dogmático, a subsidiariedade está cingida a evitar a incidência do direito penal quando existam outros mecanismos estatais menos rigorosos para a proteção do bem jurídico. Isso não inclui, todavia, condutas preventivas adotadas pela própria vítima. [397]

Nesse sentido, consoante Meliá, histórica e habitualmente esse princípio funciona como limite à intervenção do Estado no âmbito de liberdade dos cidadãos, mas não como sua obrigação de se abster por completo no tratamento de conflitos sociais graves.[398] Em verdade, a incriminação penal de determinadas condutas possui justamente o escopo de eximir os particulares de medidas de autoproteção. Caso houvesse uma abstenção estatal nesse aspecto, haveria excessiva instabilidade e desassossego social, posto que conduziria a uma sociedade alerta, defensiva e desconfiada, regredindo a fases prévias do contrato social.

Do mesmo modo, Meliá tece críticas ao princípio vitimológico, notadamente quanto aos conceitos de merecimento e necessidade de proteção penal. Isso porque não se pode identificar um fundamento material de sua influência sobre a noção de bem jurídico. Adeptos da corrente minoritária não apresentam definição clara acerca de quem "merece" ou "necessita" de

[397] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, pp. 564-565.
[398] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal.* Tese de Doutorado. Universidad Autónoma de Madrid, 1997, pp. 388-389.

proteção, limitando-se ao raciocínio de que o titular do bem poderia ter evitado o resultado. Esse raciocínio, sem maiores desenvolvimentos, conduz a uma simples penalização da vítima, desvirtuando os fins do direito penal.[399] Por essa razão, recorrer à autorresponsabilidade, limitada à noção de autonomia lastreada no contrato social, porém sem acréscimo de conteúdo ao conceito, é inócuo para a sedimentação de uma teoria vitimodogmática.[400]

Disso decorre que a corrente minoritária não justifica a partir de qualquer princípio penal, expresso ou implícito, a razão pela qual a negligência da vítima implique seu desmerecimento de proteção, visto que com a lesão ela não consente.[401]

Por essa razão, a carência de respaldo legislativo ou dogmático é uma crítica frequentemente aventada, posto que o emprego dos postulados vitimodogmáticos não possuiria qualquer fundamentação normativa. Aponta-se para uma desconexão dos institutos dogmáticos, afastando-se dos postulados da parte geral e de vários delitos da parte especial – considerando uma aplicação centrada no delito de estelionato e poucos crimes patrimoniais-, o que não é resolvido pelo simples emprego da interpretação teleológica.[402] Por conseguinte, torna-se insustentável uma formulação do princípio vitimológico com pretensões generalistas.

As críticas tecidas a essa corrente também merecem procedência na seara de crimes informáticos. A aplicação dos conceitos de merecimento e necessidade de proteção no ambiente informático importaria em raciocínio demasiadamente fluido. Emerge uma imprescindibilidade de empoderamento dos usuários, porém não uma atribuição desmedida de responsabilidades virtuais hercúleas. Como ponderado por Crespo, é preciso distinguir hipóteses de negligência ou imprudência dos usuários daquelas em que há efetivo consentimento do ofendido, posto que apenas este conta com uma voluntária e consciente adesão ao resultado.[403] Assim, uma total e indistinta ausência de responsabilização nessas hipóteses importaria em uma postura informática excessivamente defensiva dos usuários, prejudicial ao exercício e fomento do bem jurídico tutelado, bem como obstativo de inovações nesse ambiente.

A partir da compreensão das teorias criminológicas aplicáveis ao ambiente virtual, depreende-se que as vítimas descuidadas, gananciosas e solitárias enquadram-se nos principais perfis suscetíveis aos crimes informáticos, de modo que um total abandono de sua tutela seria

---

[399] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal.* Tese de Doutorado. Universidad Autónoma de Madrid, 1997, pp. 398-400.
[400] LUZON PENA, Diego-Manuel. Principio de Alteridad o de Identidad vs. Principio de Autorresponsabilidad. Participacion en Autopuesta en Peligro, Heteropuesta en Peligro Consentida y Equivalencia: El Criteria del Control del Riesgo. *Nuevo Foro Penal*, v. 74, n. 6, p. 58-80, 2010, pp. 67-68.
[401] Ibidem, pp. 67-68.
[402] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 382.
[403] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, pp. 107-108.

pouco recomendável para fins preventivos e de pacificação social, levando-se a uma inaplicabilidade prática de diversos tipos penais. Ademais, a corrente minoritária levaria a uma desconsideração por completo do efeito desinibidor desencadeado pela Internet sobre os usuários, em violação ao princípio da culpabilidade.

Sob o viés informático, a incidência do princípio da subsidiariedade deve se voltar a outros mecanismos jurídicos e políticas públicas, como se depreende das posturas fomentadas pela *situational crime prevention*. Destaca-se o aprimoramento legislativo das disposições do Marco Civil da Internet – expandindo-se a responsabilidade civil de provedores de Internet, a título exemplificativo – e a educação digital dos usuários, de modo a mitigar os fatores de vulnerabilidade e fomentar efetiva compreensão do aspecto vitimodogmático dos usuários por meio de uma mitigação dos fatores intrínsecos (psicológicos) e extrínsecos (carência de regulamentação e investigação) alheios à autodeterminação informática. Referida realidade, contudo, não deve implicar abandono indistinto da tutela penal, à contrariedade do sentido apontado pela corrente minoritária vitimodogmática. Em verdade, trata-se de medidas concomitantes à tutela penal e à compreensão da vítima no fenômeno delitivo informatico, o que apenas reforma a inaplicabilidade do princípio da subsidiariedade – agora visto sob o viés informático – à vitimodogmática.

Apesar das críticas tecidas a essa corrente vitimodogmática, não se pode olvidar a contribuição essencial para reinserir a vítima como sujeito central junto do autor na prática delitiva, bem como reforçar os princípios corolários do direito penal. Contudo, outros autores apontam para soluções matizadas e alternativas, que possibilitam melhor adequação da vitimodogmática à teoria geral do delito.

5.2.3. Síntese das correntes

As críticas tecidas à corrente minoritária não são refutadas com propriedade por seus defensores. O princípio vitimológico, por si, não denota conteúdo suficiente para sustentar a tese de desmerecimento e desnecessidade de proteção da vítima: há uma lacuna que não revela por que nessas hipóteses inexistiria lesão ao bem jurídico tutelado. No cerne da questão: à luz da atual dogmática penal, não se confere uma explicação para a atipicidade de condutas comissivas dolosas do autor face a uma atitude culposa do ofendido.

Nesse ponto, o princípio da subsidiariedade, por si, não é apto a sustentar uma atipicidade indiscriminada, visto que levaria a uma perda de proteção penal, com consequente desassossego social. Logo, como expõe Silva Sánchez, a adoção de medidas ativas de

autoproteção não pode ser exigível usualmente, visto que o monopólio da força recai sobre o Estado, a quem incumbe a proteção dos cidadãos, em regra.[404] Com isso, a corrente minoritária carece de lastro constitucional ao promover uma interpretação inadequada da noção de subsidiariedade do direito penal.

Por outro lado, a simples adoção da corrente majoritária mostra-se muito tímida diante da importância que o papel da vítima é apto a desempenhar, inclusive quanto aos crimes informáticos. A falta de previsão legal, por si só, não constitui óbice para o desenvolvimento da teoria do delito, como assim ocorre com diversos institutos, como o princípio da insignificância e o consentimento do ofendido.

Ademais, Schünemann apresenta correta oposição ao paternalismo penal, em defesa da autonomia individual, cujas bases se originam no contrato social. A Constituição Federal pressupõe que o ser humano possui capacidade de autodeterminação, que apresenta como pressuposto lógico a noção de responsabilidade pessoal, atribuindo-se responsabilidade apenas por atos próprios.[405]

Como aponta Cabette, muito embora haja intenso debate doutrinário quanto a correntes mais ampliativas da vitimodogmática, justamente porquanto o direito penal em regra veda a compensação de culpas e remanesce o desvalor da ação, é bem verdade que haverá reduzido ou ínfimo desvalor do resultado a depender do grau de culpa na omissão de proteção da vítima.[406] Cite-se, como exemplo emblemático, a hipótese de torpeza bilateral, em que o usuário também atua contrariamente aos ditames de boa-fé.

A partir desse raciocínio, em regra, o autor não responderá por comportamentos alheios. Por essa razão, Meliá entende que o princípio da autorresponsabilidade adquire relevância, porém não lastreado no critério necessidade/merecimento de proteção da vítima. Com fundamento no livre desenvolvimento do indivíduo, o autor propõe a associação de duas perspectivas: autonomia e responsabilidade, ou seja, todo cidadão possui um âmbito de organização própria de seu âmbito vital e a ele compete a responsabilidade por danos causados por sua organização própria.[407] Para tanto, à contrariedade de Schünemann, Meliá sustenta que haverá incidência do princípio da autorresponsabilidade quando a atividade realmente possa ser

---

[404] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 177.
[405] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 446.
[406] CABETTE, Eduardo Luiz Santos. Torpeza ou fraude bilateral no estelionato sob a ótica da vitimodogmática e da autoproteção. *Revista Síntese de direito penal e processual penal*, Porto Alegre, v. 19, n. 115, p. 59-63, abr./mai. 2019. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=150328. Acesso em: 6 jan. 2021.
[407] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 449.

atribuída à vítima, ou seja, diante de sua ciência acerca dos riscos e/ou da previsibilidade do resultado lesivo.

Para uma adequada imputação, Meliá entende ser necessária uma lógica estruturação da autorresponsabilidade na teoria do delito. Desenvolve, dessa maneira, a teoria de imputação à vítima, de modo a inserir referido raciocínio na teoria da imputação objetiva, como se verá no Capítulo 6.2.2. (Imputação à vítima de Cancio Meliá). Assim, diferentemente de Schünemann e outros defensores da vitimodogmática, Meliá defende a inserção da autorresponsabilidade em com base em critérios normativos de imputação.[408]

A par de autores que tecem considerações vitimodogmáticas no âmbito da teoria geral do delito, parte significativa da doutrina entende ser possível conferir certa autonomia aos institutos vitimodogmáticos como critério de interpretação das disposições da parte geral e especial, inclusive como mecanismo de exclusão da tipicidade, porém em postura matizada.

Silva Sánchez defende a adoção de uma postura vitimodogmática intermediária entre uma recorrente atipicidade e a simples atenuação da pena diante de condutas descuidadas, negligentes ou gananciosas da vítima. Para o autor, o direito penal não poderá impor sanções caso a conduta do autor, por si, não contenha perigo relevante ao bem jurídico tutelado, tendo adquirido esse caráter danoso apenas em decorrência de certo comportamento da vítima. Fundamenta, contudo, essa noção vitimodogmática na fragmentariedade e proporcionalidade, e não na subsidiariedade penal. Isso porque o comportamento culposo da vítima é apto a retirar essencialmente a gravidade do fato (fragmentariedade), bem como ao autor não poderia ser imputado exclusivamente o curso causal, sob pena de exacerbação de sua responsabilidade (proporcionalidade) e consequente violação do princípio da culpabilidade.

Para esse autor, não incumbe apenas ao legislador, mas também ao intérprete, a tarefa de selecionar quais as condutas mais gravosas que carecem de sanção penal. Dessa forma, uma conduta típica em interpretação meramente gramatical poderá ser excluída a partir de considerações teleológicas, posto que limitadas ao campo conceitual (*Begriffshof*). Um direito penal mínimo permite restrições ao alcance do tipo, como ocorre a partir de noções doutrinária e jurisprudencialmente desenvolvidas, como a adequação social e o risco permitido. Aliás, seu

[408] Nesse ponto, a autocolocação em risco e a heterocolocação em risco consentida, inseridas por Roxin no bojo da teoria da imputação objetiva, também guardam correlação com a noção de autorresponsabilidade e atribuição de riscos. Verifica-se, assim, que há aportes da vitimodogmática sobre a teoria da imputação objetiva, que será analisada em Capítulo próprio.

uso adequado não gera prejuízos à pacificação social, mas fomenta a solução dos conflitos sociais por outros mecanismos do ordenamento, à margem do direito penal.[409]

À contrariedade daquilo defendido pela corrente minoritária vitimodogmática, Silva Sánchez propõe que condutas descuidadas e imprudentes da vítima, em geral, não culminarão com atipicidade da conduta do autor. Em verdade, eventual responsabilidade apenas será atribuída exclusivamente à vítima quando, ante um risco concreto e relevante, ela opta por se expor. Logo, excluem-se riscos abstratos de modo que, apenas em uma situação concreta de perigo ao bem jurídico, se o titular não adotar medidas mínimas de cautela, o processo lesivo dos bens estará em seu âmbito de responsabilidade.[410_411]

Silva Sánchez apresenta três principais motivos para a fundamentação desse raciocínio, objetando-se às críticas a ele aplicáveis: a) não haverá desconfiança social caso se trate de medidas de proteção usuais e razoáveis diante de riscos identificados pela vítima; b) não há vitimização, mas adequada atribuição de responsabilidade ao autor, sem colocar riscos pertencentes à esfera de organização alheia; c) há uma tendência ao surgimento de institutos despenalizadores pela doutrina, como os princípios da insignificância e adequação social.[412]

Dever mais evidente imposto à vítima consiste em não realizar conscientemente atos que culminem com uma criação ou incremento de risco de lesão de bens jurídicos de sua titularidade, notadamente caso a lesão pressuponha ato comissivo ou omissivo seu (na linha da classificação de delitos de relação proposta por Schultz). Exemplo notório proposto por Silva Sánchez é a hipótese de estelionato bilateral: caso a vítima não esteja em plena situação de erro, mas apenas incida em dúvida acerca da proposta do agente, não haverá necessidade de proteção (*Schutzbedürftigkeit*), posto que adquire feição de um negócio aleatório.[413]

---

[409] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 176-177.

[410] Ibidem, p. 178.

[411] Conforme propõe o autor espanhol, esse enfoque vitimodogmático se amolda adequadamente à teoria do delito. Afinal, ao conferir atenção ao comportamento da vítima diante do risco concreto, pode-se concluir que a conduta do autor não era qualitativa (inserindo-se no risco permitido ou âmbito do consentimento) ou quantitativamente (baixo ou ínfimo risco) relevante. Embora um risco *ex ante* seja potencialmente lesisv ao bem jurídico, mostra-se irrelevante sob a perspectiva *ex post* em razão da conduta da vítima. Esse raciocínio, aliás, também é aplicado pela teoria da imputação objetiva (visto que o risco abstrato, *ex ante*, deve se manifestar no resultado, *ex post*). (SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, pp. 178-179).

[412] Nessa linha, o autor traz exemplo já consagrado na jurisprudência acerca da repercussão da omissão da vítima sobre a responsabilidade do autor, impondo-se certo dever ativo de proteção ao ofendido: caso o autor tenha causado lesões corporais leves, impõe-se a adoção pela vítima de medidas curativas medicinalmente esperadas; caso contrário, se a ferida se expandir por falta de cuidados, eventual lesão corporal grave ou mesmo a morte não serão imputadas ao autor (SILVA SÁNCHEZ, José María. *Op. cit.*, pp. 180-182).

[413] A hipótese do estelionato bilateral será retomada quando da análise do funcionalismo penal no Capítulo 6.5.1. (SILVA SÁNCHEZ, José María. *Op. cit.*, p. 183).

Em razão das diversas críticas tecidas à corrente minoritária, Schünemann também busca matizar seu entendimento, alinhando-o significativamente àquele esposado por Silva Sánchez, salvo no tocante à manutenção do princípio da subsidiariedade como fundamento para a vitimodogmática. Nesse sentido, o autor alemão sustenta que a credulidade e leviandade da vítima, em se tratando de estelionato ou fraude, não implicarão exclusão do tipo penal, mas tão somente se se estiver diante de uma dúvida concreta apta a excluir o erro da vítima, afastando uma elementar do tipo penal.[414]

A seu turno, alinhando-se a Schünemann em caso de atuação da vítima mediante engano idôneo, Arzt e Weber sustentam que remanesce a punibilidade a título de tentativa de estelionato, visto que uma completa irresponsabilidade do autor não seria admissível sob a ótica político-criminal. Afinal, considerando que houve início dos atos executórios, resta configurada a tipicidade da conduta, muito embora sua consumação tenha ocorrido em razão da postura desidiosa adotada pela vítima.[415] Com essa postura, confere-se viés moderado à posição minoritária, de modo a não retirar a proteção penal sobre vítimas descuidadas e negligentes, como inicialmente sua teoria levava a crer.

Em linhas gerais, no entendimento de Silva Sánchez, com o qual se compactua, e de Schünemann (com a ressalva acerca da fundamentação de sua proposta vitimodogmática): a) a ótica vitimodogmática apenas incide em hipóteses nas quais a vítima possui ciência ou estava em condições de saber acerca da existência de um risco concreto ao bem jurídico; b) em se tratando de estelionato, caso mais emblemático, ou qualquer delito permeado por engodo/fraude, se o engano provocado pelo autor não é suficiente a produzir erro sobre a vítima, a conduta será atípica por se tratar de tentativa impossível, ainda que o resultado tenha se produzido, por se inserir no âmbito de responsabilidade do sujeito passivo (como na hipótese de estelionato bilateral); c) se o engano for suficiente para provocar o engano, porém a vítima toma ciência do risco concreto ou estava em condições de sabê-lo, haverá rompimento do nexo de causalidade, respondendo o autor exclusivamente por tentativa, capitulação jurídica em nada maculada pelo resultado meramente naturalístico.[416] Referidas conclusões, em certa medida

---

[414] Isso porque, dado o caráter dúplice do engano, como aponta Schünemann, seria um contrassenso reconhecer a existência de erro caso uma pessoa possua dúvida: o indivíduo decide consciente dessa insegurança, de modo que atua como um *homo oeconomicus* em negócio aleatório. (SCHÜNEMANN, Bernd. El sistema del ilícito jurídico-penal: concepto de bien jurídico y victimodogmática como enlace entre el sistema de la parte general y de la parte especial. In: HERNÁNDEZ, Moisés Moreno (Coord.). *Problemas capitales del moderno derecho penal a principios del siglo XXI*, Editorial Ius Poenale, México D.F., pp. 87-113, 2003, p. 117).

[415] Ibidem, p. 127.

[416] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, p. 184.

convergem com os postulados apresentados sob a ótica da teoria da imputação objetiva, como se verá no Capítulo 6 (Funciomalismo penal e a vítima nos crimes informáticos).

Com isso, o cerne dessa teoria vitimodogmática consiste em identificar a noção de risco ou perigosidade da conduta, ou seja, sua aptidão a enganar a vítima. Um critério objetivo de risco pode conduzir a uma amplitude exacerbada, lastreada no conceito de cidadãos médios, homem de prudência média. Por outro lado, um excessivo critério subjetivista tornará inócua a noção de autorresponsabilidade e fragmentariedade, eis que o erro seria a demonstração de que a conduta do autor gerou um risco. Por essa razão, Silva Sánchez aponta para uma tendência à objetivização (por meio de critérios mínimos pré-fixados), com matizes subjetivas (considerando-se o sujeito passivo no caso concreto).[417]

5.3 Vitimodogmática e crimes informáticos

Os aportes da corrente vitimodogmática majoritária mostram-se excessivamente limitados e fortemente dependentes de alterações legislativas para maior grau de concreção. Ocorre que, como apontam os estudos vitimológicos, o papel desempenhado pela vítima adquire, notadamente na sociedade de risco, posição central juntamente com a conduta do autor do delito em observância aos princípios da culpabilidade e da intervenção mínima.

O princípio da autorresponsabilidade, derivado do contrato social e plasmado na Constituição Federal, é um critério interpretativo relevante, o qual já influenciou a criação de outros institutos na seara penal, como o consentimento do ofendido. Seus aportes são fundamentais para o desenvolvimento da teoria da imputação objetiva – notadamente autocolocação em risco,[418] porém não devem se limitar à teoria do delito, trazendo contribuições sobre a interpretação dos tipos penais específicos.

A tese sustentada por Silva Sánchez, ao lastrear a vitimodogmática na autorresponsabilidade e fragmentariedade penal, permite uma correção da corrente minoritária capitaneada por Schünemann, afastando-se de conceitos abstratos de necessidade e merecimento de proteção, derivados da subsidiariedade penal. O autor espanhol traz a importância do papel da vítima, a partir de hipóteses de estelionato, para delimitar hipóteses de

---

[417] SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria do delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v. 34, pp. 184-185.

[418] De fato, o princípio da autorresponsabilidade adquire relevo no terceiro elemento da teoria da imputação objetiva, qual seja, o alcance do tipo penal. (PEREZ MANZANO, Mercedes. Acerca de la Imputación Objetiva de la Estafa. In: *AA.VV., Hacia un Derecho Penal Económico Europeo*, Madrid: BOE, 1995, p. 292).

não incidência penal: a) cria novas perspectivas para compreensão crimes impossíveis quando praticados mediante fraude ou engodo, não mais lastreados na consumação concreta do delito, mas em condutas objetivas esperadas e exigíveis do sujeito passivo; b) considera o papel subjetivo da vítima, quando ciente dos riscos, como apto a eximir o autor da atribuição da modalidade consumada do delito.[419] Nesse sentido, essa síntese entre as correntes majoritária e minoritária reporta diretamente ao lastro constitucional do livre desenvolvimento da personalidade, de modo que a assunção de riscos também se consubstancia em uma manifestação do exercício do bem jurídico-penal.

Convém ressaltar que as contribuições da vitimodogmática não se limitam ao delito de estelionato, delito de relação por excelência, mas sempre que, em se tratando de bens jurídicos disponíveis, pressuponha-se algum grau de atuação da vítima para a consumação do delito. Por essa razão, são aplicáveis à luva os ensinamentos vitimodogmáticos aos crimes informáticos que pressuponham uma interação ativa do usuário. Como visto, nessas hipóteses a conduta da vítima é determinante para a consumação da maioria dos delitos no meio virtual, de modo que deve influir sobre a atribuição de responsabilidade ao autor.

À toda evidência, os aportes vitimodogmáticos atingem delitos informáticos próprios, como a invasão de dispositivo informático, além de impróprios, como estelionato, fraude eletrônica e furto mediante fraude por meio de dispositivo informático ou eletrônico. Aliás, a própria iniciativa da ação penal em parte desses delitos denota referida constatação: para os delitos de estelionato e invasão de dispositivo informático, em regra, a iniciativa será pública condicionada à representação do ofendido, a reforçar a importância preeminente do bem jurídico sob a ótica individual.

A corrente vitimodogmática matizada por Silva Sánchez, nesse contexto, mostra-se compatível com as principais teorias criminológicas emergentes na seara informática. Com efeito, a partir da teoria das atividades rotineiras, surgem elementos relevantes atrelados à conduta da vítima do ambiente virtual. Para a prevenção delitiva mostra-se importante o incremento de guardiães capazes, consubstanciados pelo uso adequado de mecanismos de segurança (*firewalls*, *antimalwares*, atualização constante do dispositivo informático). Ademais, a fim de se reduzir a adequação do alvo, na linha do acrônimo IVI (trinômio inserção do bem-valor-interação) proposto por Miró Llinares, impõe-se um estilo de navegação virtual

[419] Verifica-se, outrossim, que esses critérios recebem contornos mais claros com o desenvolvimento da teoria da imputação objetiva, de modo que sua contribuição se mostra profícua para o desenvolvimento da vitimodogmática nos moldes propostos por Silva Sánchez.

diligente, impondo-se interação cuidadosa do usuário no ambiente virtual, com vistas a mitigar o fator "interação". Uma negligência do usuário na adoção dessas medidas culminaria com a incidência do raciocínio vitimodogmático em razão da autorresponsabilidade do usuário no ambiente virtual.

Nesse sentido converge a teoria da prevenção situacional do crime, ao propugnar a necessidade de aumento do esforço percebido pelo agente quando da prática delitiva, sendo central o papel do usuário por meio da adequada instalação de mecanismos de segurança, emprego de senhas fortes e outros elementos. Assim, caso a vítima não tenha desempenhado seu papel razoável de incremento de esforço percebido pelo agente, verificam-se igualmente implicações vitimodogmáticas à luz da autorresponsabilidade e fragmentariedade penal.

Quanto ao ponto, a teoria da prevenção situacional do crime viabiliza uma delimitação negativa da área de incidência de elementos vitimodogmáticos, a impor a configuração penalmente típica em determinadas situações. Por certo, ao suscitar a importância da educação digital dos usuários, atribui-se essa tarefa ao ente estatal, de modo a mitigar o princípio da autorresponsabilidade sob o prisma individual – o que repercute sobretudo nas vítimas ignorantes, que devem receber maior tutela pelo ordenamento penal. Referidas ponderações confluem para uma adequada composição da teoria vitimodogmática nos delitos informáticos, evitando-se excessiva vitimização de usuários vulneráveis.

Do mesmo modo, a teoria da prevenção situacional do crime delineia um quadro de atuação estatal conjunta nas esferas cível, administrativa, além de incremento investigativo e atuação transnacional na prevenção delitiva. Disso decorre que nem todas as condutas tidas por negligentes devem ser afastadas aprioristicamente da tutela penal sob o rótulo de incidência da autorresponsabilidade vitimodogmática – ainda que sua incidência ocorra de forma matizada. Assim, neste ponto se encontram os contornos positivos do princípio da fragmentariedade, em que se impõe a tutela penal nos moldes do Estado Democrático de Direito para adequado fomento dos bens jurídicos disponíveis em tela: a autodeterminação informática e o patrimônio.

A par de se deixar permear por critérios objetivos delineados pelas teorias criminológicas emergentes, a proposta vitimodogmática de Silva Sánchez também viabiliza a consideração de parâmetros subjetivos no caso concreto, recebendo sua legitimidade a partir dos principais perfis de vítimas informáticas (delineados no Capítulo 4.4. (Proposta de classificação das vítimas informáticas). Logo, haverá presunção de vulnerabilidade de vítimas idosas (que já recebem tutela penal específica por meio de previsão de agravante) e jovens

(crianças e adolescentes, mais ingênuos e suscetíveis a atividades arriscadas na Internet em razão de sua tenra idade).[420]

Na esteira da teoria da prevenção situacional do crime, a tutela penal adota viés mais protetivo à vítima ignorante, sobre a qual a autorresponsabilidade vitimodogmática recai de forma matizada, com vistas a evitar a culpabilização de usuário que não possui conhecimentos técnicos bastantes para a prevenção delitiva. Como aponta Tangerino, a heterogeneirdade das vítimas na seara dos delitos informáticos, notadamente quanto à informação sobre o comportamento virtual, enseja a adoção de políticas de educação tecnológica.[421] À medida que se conscientizem, assim, os usuários não podem alegar "sumária ingenuidade", devendo adotar postura ativa em sua proteção na sociedade de risco. Nessa esteira, para vítimas solitárias, curiosas, descuidadas e gananciosas, para as quais a princípio não há exploração de fraqueza técnica, é possível traçar condutas dignas de reflexão, nas diretrizes esboçadas a seguir.

Assim, será possível se cogitar de: a) exclusão de tipicidade da conduta, caso o erro ou engano configure crime impossível que a vítima gananciosa leva a cabo em busca de lucro fácil, a partir de condutas elementares legitimamente exigíveis dos usuários; b) responsabilização do autor somente por tentativa, caso o usuário possua ciência do risco concreto de sua conduta de navegação na *web* ou *darkweb*, ou mesmo fornecimento desidioso de dados e valores, como na hipótese de vítimas curiosas e descuidadas; c) atenuação da pena do autor, diante de conduta negligente da vítima, nos termos do artigo 59, do Código Penal, como na exploração de vítimas solitárias em sites de relacionamento. Delineia-se, nesse esteio, uma gradação entre diligências: a) essenciais; b) razoavelmente exigíveis das quais o usuário possui ciência; c) esperadas do usuário médio.

De início, exemplos emblemáticos para uma integral atipicidade da conduta por se tratar de crime impossível dizem respeito ao engodo manifestamente fraudulento. Para os delitos de fraude eletrônica e estelionato, não se deve reconhecer preenchido o tipo penal caso a vítima, movida por ganância, forneça dados pessoais ou transfira valores em razão de e-mails excessivamente sensacionalistas (como no notório "golpe da herança" ou "golpe do bilhete

[420]Como se exporá em maiores detalhes no Capítulo 6.5, trata-se de presunção relativa de vulnerabilidade, que poderá ser elidida no caso concreto caso se apurem conhecimentos informáticos bastantes da vítima jovem ou idosa.

[421]A (in)aplicabilidade da tese da autocolocação da vítima em risco aos delitos perpetrados por meio das novas tecnologias. *In: ESTUDOS em homenagem a Vicente Greco Filho.* Organização de Renato de Mello Jorge SILVEIRA, João Daniel RASSI. São Paulo: LiberArs, p. 101-107, 2014, p. 101. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=111521. Acesso em: 13 set. 2020.

premiado") ou de produtos oferecidos por preço vil (em leilões de automóveis ou anúncios, por exemplo).[422]

Tratando-se do usuário de conhecimento informático médio, cogita-se singelamente de tentativa diante da conduta formalmente típica de invasão de dispositivo informático desprovido de mecanismos de segurança – conforme a redação dada pela Lei n. 14.155/21 – quando o usuário descuidado voluntariamente desativa o *firewall*, o qual, caso ativo, certamente obstaria o ataque. Todos esses elementos, todavia, deverão ser comprovados mediante perícia.

Uma responsabilização do autor pela modalidade tentada dos delitos previstos nos artigos 154-A e 155, §4º, inciso 2-B, do Código Penal, pode ser concebida quando os usuários busquem acessar a *darkweb* sem as devidas cautelas (vítima curiosa), tendo em vista a alta plausibilidade de invasão do dispositivo. Particularmente quanto ao delito de furto mediante fraude por invasão de dispositivo informático, postula-se a modalidade tentada do delito quando um usuário ingressa em seu *Internet Banking* por meio de rede pública ou lan-houses, inclusive porque se trata de diligências amplamente desaconselhadas em noticiários e por instituições financeiras.

Como visto, caso o indivíduo efetue voluntariamente o *download* de determinado *malware*, ainda que submetido a erro, não se perfaz o delito de invasão de dispositivo informático. Caso a finalidade ulterior seja a prática de furto, como na instalação de *keylogger* ou *screenlogger*, é viável incidir exclusivamente a modalidade tentada do delito se o usuário anuiu com o download de arquivo proveniente de anúncio sensacionalista, ou de publicidade irreal (como anúncios de "emagreça 10 quilos em uma semana" ou "ganhe 1000 reais por dia sem trabalhar").

A tentativa também pode ser considerada em casos concretos de fraude eletrônica e estelionato a partir de mensagens e e-mails de origem desconhecida, caso haja certo grau de plausibilidade em seu conteúdo, porém o usuário não adote ulteriores medidas para verificar sua veracidade. A título exemplificativo, a receber uma cobrança desconhecida de uma instituição financeira em que possui conta corrente, o indivíduo a paga imediatamente, sem adotar outras diligências. Do mesmo modo, caso o indivíduo adquira produtos em sites desconhecidos, por valor inferior ao de mercado (porém não por preço vil), sem prévia consulta da presença de HTTPS em sua URL e de informações sobre a fiabilidade do site.

Ainda, é possível a incidência do artigo 59, do Código Penal, diante de condutas dotadas de algum grau de negligência dos usuários. Cite-se, a título exemplificativo, o indivíduo que

[422] Mais detalhes no Capítulo 6.5.1. (Caso emblemático da torpeza bilateral).

deixa de atualizar seu antivírus instalado ou utiliza senhas fracas de proteção. Também pode-se refletir acerca do usuário de sites e aplicativos de relacionamentos (vítima solitária) que, iludido, fornece dados ou valores a pessoa desconhecida.

Por fim, muito embora a vitimodogmática tenha um caráter preponderantemente voltado à redução da responsabilidade do autor em razão da conduta da vítima, deve-se ponderar o reverso da moeda para uma holística aplicação da dogmática penal. Afinal, para fins criminológicos, mostra-se adequado um incremento de pena quando se está diante de vítima diligente: a teoria das atividades rotineiras e a prevenção situacional do crime apontam para uma relação inversamente proporcional entre grau de diligência da vítima e incidência de crimes informáticos, de modo que os cuidados no ambiente virtual devem ser fomentados. A seu turno, caso um usuário diligente seja vítima de um delito informático, nota-se maior grau de sofisticação da fraude, o que ensejará maior reprovabilidade concreta de sua conduta. Destarte, *a contrario sensu*, deve-se refletir acerca da inclusão de causas de aumento de pena ou agravante quando se está diante de vítimas diligentes.

Do mesmo modo, caso o agente tenha por alvo vítimas presumidamente vulneráveis, como idosos e jovens com idade inferior a 14 anos, um incremento da pena mostra-se recomendável para a tutela desses grupos, com destaque para os jovens, mais suscetíveis a crimes informáticos conforme delineado pela teoria das atividades rotineiras. Frise-se a possibilidade de rechaço dessa presunção, caso se trate de vítima com conhecimentos informáticos elevados no caso concreto. Referido aumento encontra-se presente em partes, e de forma genérica, na atual agravante do artigo 61, inciso II, alínea “h”, do Código Penal.

Assim, com o reconhecimento da viabilidade de incremento de pena em determinadas circunstâncias, procede-se a uma análise coerente com as teorias criminológicas na seara informática e compatível com a vitimodogmática, viabilizando-se uma compreensão holística da vítima e integral aplicação da teoria geral do delito. Referidos aportes vitimodogmáticos aos crimes informáticos podem ser harmonizados com os postulados funcionalistas, considerando-se a importância do princípio da autorresponsabilidade na construção de ambas as teorias. No entanto, enquanto o funcionalismo busca maior grau de normatização, a vitimodogmática traz maiores necessidades de análise do tipo penal específico. De qualquer modo, a análise casuística é marcante nesse escrutínio. A seu turno, nada obsta a aplicação isolada de um ou outro, porquanto dotadas de independência científica de seus postulados. Logo, a vitimodogmática é plenamente aplicável por teorias finalistas.

6. FUNCIONALISMO PENAL E A VÍTIMA NOS CRIMES INFORMÁTICOS

Neste Capítulo busca-se demonstrar a relevância da conformação dos delitos informáticos ao funcionalismo penal de modo a trazer um novo elemento aglutinador aos postulados constitucionais, vitimológicos e vitimodogmáticos já vislumbrados.

Paralelamente à vitimodogmática, as propostas funcionalistas reconhecem o valor constitucional do livre desenvolvimento do indivíduo como manifestação da autodeterminação humana. Assim, a construção das teorias funcionalistas de imputação perpassa pelo reconhecimento do âmbito de organização da vítima, que se torna protagonista na prática delitiva. Inclusive o funcionalismo sistêmico de Jakobs, como se verá, trata dos papéis sociais dos indivíduos em sociedade com lastro na autorresponsabilidade.

Na sociedade de risco, assim, o funcionalismo também destaca o aspecto positivo do exercício das liberdades como decorrentes da dignidade humana, o que reverbera sobre os bens jurídicos ora analisados: autodeterminação informática e o patrimônio.

Com isso, busca-se demonstrar que as teorias funcionalistas convergem para conferir maior relevância à conduta da vítima na conformação penalmente típica, o que também repercute sobre os delitos informáticos, manifestando-se sob os aspectos de autocolocação em risco (Segundo Claus Roxin), ações a próprio risco (conforme a teoria sistêmica de Jakobs) e na teoria de imputação à vítima (conforme entendimento de Cancio Meliá).

A partir do enfoque sobre o funcionalismo moderado de Claus Roxin, que recorre à critérios constitucionais e político-criminais como regentes da dogmática penal, mune-se dos influxos criminológicos na seará informática delineados no Capítulo 3 para determinar as repercussões penais da assunção de condutas arriscadas pelos usuários no ambiente virtual.

6.1.Funcionalismo penal

De início, promove-se breve análise acerca do surgimento e dos fundamentos do funcionalismo penal, a fim de evidenciar a pertinência de sua incidência sobre os crimes informáticos.

Considerando a contribuição do progresso científico-filosófico para o Direito Penal, inicialmente postulou-se um classicismo jusnaturalista como reflexo de um momento "pré-científico", como alcunhado por positivistas. Com o advento do positivismo, buscou-se reforçar o caráter científico da ciência penal. O neokantismo, a seu turno, ampliou a limitada concepção positivista sobre o conceito de ciência, expandindo a noções de ciências culturais e do espírito

com vistas a superar o excessivo formalismo do modelo predecessor. O finalismo, por fim, buscou superar o subjetivismo desencadeado pelo neokantismo, recorrendo aos objetos reais.[423]

Em oposição ao neokantismo, para Welzel, a ação não tem natureza meramente causal, mas visa a determinado fim, porquanto o homem pode prever, na medida do possível, as consequências de suas ações. Nesse sentido, o homem é capaz de direcionar o acontecer causal para determinado fim almejado, distinguindo-se essa ação de uma simples acontecer causal, proveniente de uma série de fatores concomitantes de cada caso.[424] Nessa linha de raciocínio é possível estabelecer uma legalidade da ordem ético-social, porque os mandamentos dirigidos ao homem sempre devem apresentar um conteúdo referente a ações finais.[425]

O pensamento funcionalista no último trintídio do século XX desponta em razão de críticas traçadas ao finalismo, cujo aspecto lógico-objetivo ainda se mostrava insuficiente para fazer frente a todas as questões dogmáticas. O grande mérito de Welzel foi reconhecido e incorporado: a consideração do elemento subjetivo (dolo) quando da análise típica da conduta. No entanto, foram tecidas diversas críticas sobre os resultados propugnados para os crimes culposos, omissivos, além da concepção de que diversos institutos jurídicos estavam circunscritos a "aspectos ontológicos imutáveis".[426]

Isso porque, na opinião dos funcionalistas, a principal estrutura ontológica delineada por Welzel, qual seja, a ação final possui uma capacidade de limitação ao legislador – e, por via transversa, ao poder estatal – pouco significativa: não confere ferramentas para se delimitar o cerne da teoria do delito, vale dizer, quais ações finais devem ser consideradas ilícitos penais.[427] Logo, conforme expõe Schünemann, o finalismo superestima as consequências normativas de um dado ontológico, sobretudo na seara das ciências criminais, em que os princípios fundamentais do direito penal desempenham um papel central, porém são carecedores de conteúdo normativo.[428]

---

[423] MIR PUIG, Santiago. *Introducción a las bases del derecho penal.* Montevideo: B de f, 2. ed., 2003, pp. 276-277.
[424] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte Geral.* 19ª ed. São Paulo: Saraiva, 2012, p. 120.
[425] BUSTOS RAMIREZ, Juan. *Introducción al Derecho Penal***.** Bogotá: Editorial Temis, 2. ed, 1994, pp. 164-165.
[426] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, pp. 110-111.
[427] Destarte, como aponta Mir Puig, a teoria da imputação objetiva, a partir de postulados político-criminais é dotada de maior potencial de delimitação normativa. (MIR PUIG, Santiago. Límites del normativismo em Derecho Penal. *Revista Electrónica de Ciencia Penal y Criminologia*, v. 7, n. 18, p. 1-24, 2005, pp. 18-19).
[428] SCHÜNEMANN, Bernd. La relación entre ontologismo y normativismo em la dogmática jurídico-penal. *In:* CONGRESO INTERNACIONAL. FACULTAD DE DERECHO DE LA UNED. *Modernas tendencias em la ciencia del* derecho penal y em la criminología. Madrid: Universidad Nacional de Educación a Distancia, 2001, p. 139.

Outro relevante fundamento para o desenvolvimento de teorias funcionalistas consistiu no avanço tecnológico sem precedentes verificado na segunda metade do século XX, o que culminou com a pulverização de fronteiras nacionais, o encurtamento de distâncias e a gerência de riscos não apenas derivados da natureza, mas da própria ação humana. A partir dessas verificações, que Ulrich Beck alcunhou de sociedade de risco, não se trata de postular a inexistência de riscos previamente a esse período (os riscos caminham e acompanham o desenvolvimento da humanidade), porém se reconhece uma nova fase impulsionada por avanços científicos marcada por impacto nas relações sociais de forma globalizada. Conforme pondera Beck: os riscos produzidos não mais se limitam a um âmbito fabril ou regional, mas apresentam uma característica inerentemente globalizada, de forma a superar fronteiras nacionais e acarretam ameaças supranacionais. Assim, emana-se uma lógica de distribuição e manejamento político e cultural dos riscos.[429]

No entendimento de Merino Herrera, os riscos consistem em "consequências negativas evitáveis de certas decisões humanas".[430] Certas inseguranças não se limitam espacialmente, transbordando fronteiras e inclusive gerações. Dessa forma, a ocorrência do dano é irreversível, inexistindo forma de compensá-lo retrospectivamente. Está a se falar de bens difusos, atinentes a riscos energéticos, informáticos, econômicos, ecológicos, e outros, frequentemente ligados a uma criminalidade organizada e transnacional.[431]

Uma vez que todas as relações desenvolvidas dependem da linguagem, pode-se notar que nem todos os elementos provêm de uma realidade prévia, mas de decisões consensuais criadas a partir de convenções no agir comunicativo. Destarte, em uma sociedade de risco e globalizada, em que a linguagem se desenvolve com grande intercâmbio cultural, há o desenvolvimento e a reformulação constante de concepções jurídicas, de tal forma que não é possível admitir a existência de estruturas lógico-objetivas.[432]

De fato, não existem na realidade jurídica conceitos ontológicos unívocos. Assim, parte-se do pressuposto que ao direito não incumbe a mera descrição da realidade, mas sim a realização de valores, como o livre desenvolvimento da personalidade. E nesse contexto a

---

[429] BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. Tradução: Sebastião Nascimento. São Paulo: Editora 34, 2011, p. 16.

[430] MERINO HERRERA, Joaquín. *Tendencias de la política criminal contemporânea*. Madrid: Marcial Pons, 2018, p. 182.

[431] Nesse contexto, verifica-se que a teoria da ação final não é apta a fazer frente a lesões impingindas sobre bens jurídicos coletivos e difusos, nos quais pode haver uma pluralidade de autores e de condutas dificilmente individualizáveis, em que não se pode perquirir acerca do aspecto subjetivo de cada integrante (MERINO HERRERA, Joaquín. *Op. cit.*, pp. 183-184).

[432] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte Geral.* 19ª ed. São Paulo: Saraiva, 2012, p. 121.

valoração de conceitos é imprescindível, conferindo-lhes maior concretização e precisão a fim de se viabilizar a observância aos valores constitucionais mais caros.[433]

Com isso, o funcionalismo traz critérios normativos para viabilizar a dignidade da pessoa humana, com vistas ao livre desenvolvimento individual. Na seara dos crimes informáticos individuais, são estabelecidos parâmetros para a efetiva compreensão do exercício dos bens jurídicos autodeterminação informática e patrimônio, fornecendo-se um elemento aglutinador entre os valores constitucionais e a realidade.

Nesse contexto, na seara penal, emerge o funcionalismo com sua nova abordagem aos riscos da sociedade, concomitantemente ao saneamento das deficiências da teoria finalista.

Na seara dos crimes informáticos, o funcionalismo trará relevantes contribuições. Como visto no Capítulo 3, o ambiente virtual trouxe novos riscos à sociedade moderna, quer pela inovação da prática de crimes tradicionais, quer pela afetação de um novo bem jurídico tutelado, consistente na autodeterminação informática. A volatilidade, constante autoconstrução e carência de regulamentação da sociedade em rede impõem desafios sequer imaginados por autores finalistas.

De fato, frente a esse modelo dinâmico, a ação final conforme delineada por Welzel passa a ser superada. Em crimes informáticos que afetem bens supraindividuais propõe-se uma nova abordagem considerando-se ser necessária por vezes uma atuação preventiva, com atuação prévia à efetiva verificação do dano (que possui caráter irreversível). Ademais, em razão de seu caráter transnacional, com envolvimento de diversos agentes ao redor do mundo, o enfoque ontológico e lastreado na ação final cede espaço para a análise de riscos.

A seu turno, em se tratando de bens jurídicos individuais, enfoque da presente pesquisa, o funcionalismo traz novas ferramentas para fazer frente à dinamicidade do ambiente digital, porém simultaneamente conferindo sua normatização (o que o difere dos estudos vitimogdomáticos verificados no Capítulo pretérito). Uma teoria baseada em aspectos puramente ontológicos não se mostra apta a lidar com aspectos virtuais, que frequentemente não dizem respeito à própria natureza do "ser", mas apenas recebem uma imputação pela via normativa. E esse caminho busca concretizar os valores constitucionais decorrentes da dignidade da pessoa humana, com destaque para o livre desenvolvimento da personalidade, a fim de viabilizar efetiva compreensão do modo de exercício dos bens jurídicos no ambiente virtual.

---

[433] GRECO, Luis. Introdução à dogmática funcionalista do delito. Em comemoração aos trinta anos de "Política Criminal e Sistema JurídicoPenal", de Roxin. *Impresso do I Congresso de Direito Penal e Criminologia*. UFBA, painel "Funcionalismo no Direito Penal", 13-15 de abril de 2000, p. 18.

Embora haja uma base necessária na realidade física, o espaço informático pode e deve ser amoldado – também sob a ótica penal - a partir de parâmetros normativos, sem os quais passaria a valer a máxima de que a "Internet é terra de ninguém". Logo, muito embora seja necessário delinear limites a um viés jurídico securitário – e, portanto, de regulamentação expansiva, o que importaria em violações a liberdades individuais -, o aspecto normativo necessariamente integra e compõe o ambiente virtual. É nesse contexto que o funcionalismo penal melhor se amolda à abordagem dos crimes informáticos.

O funcionalismo moderado consiste na vertente pioneira e que recebe maior adesão doutrinária na atualidade, de modo que este será o enfoque adotado. De qualquer modo, não pode ser descartada a relevância de outras correntes funcionalistas para a compreensão do ambiente virtual e, notadamente, do papel desempenhado pela vítima, razão pela qual também se fará sua análise.

6.1.1. Funcionalismo moderado de Claus Roxin

Roxin, a partir de sua obra da década de 1970,[434] postula a introdução no sistema penal de uma relação com os fins político-criminais, a fim de se levar em conta os efeitos do Direito Penal sobre a sociedade. Desvincula-se da interpretação do Direito positivo em detrimento da consecução da política criminal adequada ao Estado Social e ao Estado de Direito. Trata-se de um instrumento teleológico funcional, uma vez que as categorias do delito se tornam instrumentos de persecução dos fins político-criminais a fim de que o Direito permaneça permeável a alterações valorativas.

Como postula Roxin,[435] uma repartição estanque do Direito Penal historicamente verificada se opõe a um diálogo com a Política Criminal. A Teoria Geral do Delito lida diretamente com problemas político-criminais, pois estes são capazes de superar o automatismo dos conceitos teóricos e assim fornecer soluções concretas mais justas.[436] Faz-se imprescindível, portanto, uma vinculação entre as decisões político-criminais e a fundamentação do sistema penal, o que propicia uma unidade sistemática.

Como apontam Hassemer e Conde, a política criminal guarda relação profunda tanto com os preceitos fundamentais da Constituição em um Estado Democrático de Direito como

---

[434] ROXIN, Claus. *Politica Criminal y estrutura del delito.* Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992.
[435] Ibidem, pp. 40-42.
[436] Ibidem, pp. 50-51.

com a realidade social. Apresenta um viés de justiça, que traça balizas claras para delimitar o conceito de bem juídico, por meio de critérios e princípios penais tradicionais (ofensividade, subsidiariedade, legalidade, entre outros).[437] No entendimento de Donini, trata-se de uma vinculação ao saber empírico, superando-se orientações meramente retóricas.[438]

Para fins de compreensão da visão funcionalista[439], adota-se a definição de política criminal proposta por Shecaira:

> A política criminal é uma disciplina que oferece aos poderes públicos as opções científicas concretas mais adequadas para controle do crime, de tal forma a servir de ponte eficaz entre o direito penal e a criminologia, facilitando a recepção das investigações empíricas e sua eventual transformação em preceitos normativos. Assim, a criminologia fornece o substrato empírico do sistema, seu fundamento científico. A política criminal, por seu turno, incumbe-se de transformar a experiência criminológica em opções e estratégias concretas assumíveis pelo legislador e pelos poderes públicos.[440]

À contrariedade do postulado clássico de Von Liszt, na fórmula de que o Direito Penal seria a barreira infranqueável da política criminal, atualmente a ciência dogmática se torna um instrumento de concretização desta.[441] De fato, a política criminal apresenta um viés mais abrangente que o Direito Penal, posto que não apenas se volta à prevenção e redução de causas da criminalidade, como também visa à mitigação de suas consequências.[442_443]

Ademais, como aponta Mir Puig, a teoria da imputação objetiva, a partir de postulados político-criminais (como os princípios da legalidade, intervenção mínima e culpabilidade) é dotada de maior potencial de limitação normativa quando comparada com o finalismo.[444] Afinal, lastrear-se pura e tão somente na realidade para a construção do conceito de ação típica não se mostra suficiente para a consecução dos fins do direito penal.

---

[437] HASSEMER, Winfried; CONDE, Francisco Muñoz. *Introducción a la criminología y al derecho penal*. Valencia: Tirant lo blanch, 1989, pp. 70-75.

[438] DONINI, Massimo et al. *El derecho penal frente al los desfíos de la modernidad*. Lima: Ara Editores, 2010, p. 115.

[439] O conceito ora delineado reforça a importância da compreensão dos aspectos criminológicos ds delitos informáticos, conforme apresentado no Capítulo 4., como forma de traçar as estratégias de enfrentamento e prevenção.

[440] SHECAIRA, Sergio Salomão. *Criminologia*. 6. ed. São Paulo: Revista dos Tribunais, 2014, p. 44.

[441] HASSEMER, Winfried; CONDE, Francisco Muñoz. *Introducción a la criminología y al derecho penal.* Valencia: Tirant lo blanch, 1989, p. 173.

[442] DONINI, Massimo et al. *Op. cit.*, p. 127.

[443] Roxin, nesse sentido, busca a adequação da Teoria Geral do Delito e de suas principais categorias, com vistas à consecução das finalidades de Política Criminal. Os tipos penais têm como função a consubstanciação do princípio da legalidade – *nullum crimen nulla poena sine lege* -, enquanto a antijuridicidade apresenta seu foco na regulação social de interesses sociais conflitantes. Por fim, a culpabilidade visa a limitar a pena, a fim da consecução da prevenção geral e especial (ROXIN, Claus. *Politica Criminal y estrutura del delito.* Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992, pp. 58-59).

[444] MIR PUIG, Santiago. Límites del normativismo em Derecho Penal. *Revista Electrónica de Ciencia Penal y Criminologia*, v. 7, n. 18, p. 1-24, 2005, pp 7-8.

Como discorre Schünemann, existem conceitos empíricos indeterminados, visto que possuem apenas um núcleo de significado, porém um extenso âmbito de aplicação. E o preenchimento de todo o campo de incidência apenas pode ocorrer mediante argumentos teleológicos, ou seja, lastreados na política criminal. Por essa razão, apesar de se afirmar que diversos conceitos empíricos são normativos, na verdade o funcionalismo busca apenas reduzir sua indeterminação.[445]

Afinal, o tipo objetivo não consiste em mera criação jurídico-normatica, posto que seleciona uma parcela da realidade naturalística e social preexistente. Desse modo, apenas a seleção das condutas consiste em uma disposição normativa, que adiciona uma valoração jurídica à realidade. No entendimento de Mir Puig, essa é a efetiva concretização do princípio da ofensividade, o qual, por sua vez, pressupõe que a descrição típica se refira a uma lesão ou risco a um bem jurídico cuja importância encontra-se previamente reconhecida pelo Direito Penal como carecedora de proteção.[446_447]

Deve-se ponderar, contudo, ser necessária efetiva consideração de fatores empíricos com amparo em estudos científicos. Do contrário, o mero uso argumentativo e retórico no funcionalismo poderá culminar com idênticos resultados, mudando-se apenas a roupagem do instrumento utilizado. Nesse sentido, Donini critica posições funcionalistas ao não trazer efetivamente dados empíricos para embasar algumas reinterpretações do sistema penal.[448]

Necessário se atentar, portanto, para uma efetiva contribuição de saberes empíricos sobre a dogmática penal, com vistas a viabilizar uma efetiva concreção dos preceitos funcionalistas de Roxin. Caso corretamente aplicado, a vantagem do funcionalismo consiste em se orientar a finalidades político-criminais para conferir maior concreção aos princípios penais, donde o tipo penal não se limita a descrever uma mera atividade final como dado ontológico, mas sim por meio de uma seleção dos valores dignos de tutela penal. Trata-se de trazer

---

[445] SCHÜNEMANN, Bernd. La relación entre ontologismo y normativismo em la dogmática jurídico-penal. *In:* CONGRESO INTERNACIONAL. FACULTAD DE DERECHO DE LA UNED. *Modernas tendencias em la ciencia del* derecho penal y em la criminología. Madrid: Universidad Nacional de Educación a Distancia, 2001, p. 137.

[446] MIR PUIG, Santiago. Límites del normativismo em Derecho Penal. *Revista Electrónica de Ciencia Penal y Criminologia*, v. 7, n. 18, p. 1-24, 2005, pp. PUIG, Santiago Mir. Límites del normativismo em Derecho Penal, cit., pp. 6-7.

[447] Consequentemente, não há propriamente uma contraposição entre as teorias finalista e funcionalista, posto que ambas partem de um pressuposto fático comum, em razão da irrenunciabilidade de consideração da realidade. A diferença entre os pensamentos é, portanto, somente gradual, tendo em vista a consideração normativa acrescentada pelo funcionalismo com o escopo de selecionar quais estruturas da realidade devem ser relevantes. (SCHÜNEMANN, Bernd. *Op. cit.*, p. 140).

[448] DONINI, Massimo et al. *El derecho penal frente al los desfíos de la modernidad*. Lima: Ara Editores, 2010, p. 285-286.

mecanismos empiricamente eficazes de prevenção delitiva, por meio de aportes político-criminais, respeitando-se as garantias formais e materiais do sistema penal.[449]

No tocante aos crimes informáticos, em especial, em que predominam elevada dinamicidade e constantes inovações, mostra-se profícua a adoção de referenciais político-criminais lastreados na realidade para a efetiva proteção dos bens jurídicos. Assim, a política criminal irá se munir de postulados criminológicos para traçar políticas públicas, legislativas e inclusive uma ótica interpretativa do direito penal informático.

Em se tratando de bens jurídicos individuais disponíveis (patrimônio e autodeterminação informática) desenvolvidos e afetados pelo ambiente informático, em razão da relevância da participação de todos os envolvidos – agente e vítima – exsurge particular pertinência dos estudos vitimológicos para a compreensão do fenômeno delitivo e sua prevenção.

Dessa forma, os estudos criminológicos emergentes conferem embasamentos empíricos concretos para a adoção de um Direito Penal funcionalista genuinamente calcado na realidade. Permitem incorporar os perfis de usuários mais vulneráveis e/ou suscetíveis de vitimização no ambiente virtual, buscando-se soluções normativas racionais: quer pela via de incremento da tutela penal (vítimas idosas e jovens) e da educação digital extrapenal (vítimas ignorantes), quer pela aplicação da teoria da imputação objetiva com vistas a uma mitigação da pena (vítimas curiosas, solitárias, descuidadas) ou completa atipicidade penal (vítimas gananciosas), sempre se voltando a estratégias fomentadoras de finalidades preventivas e de minoração das consequências do delito.[450]

Com isso, a seleção normativa viabilizada pelo funcionalismo, lastreada nos indicativos político-criminais, permite direcionar as condutas desejadas no ordenamento. Se, por um lado, se torna criminologicamente desaconselhável um total desamparo penal do usuário informático,[451] por outro, não se pode incentivar condutas negligentes e displicentes no ambiente informático, o que seria contraproducente sob a ótica empírica. Não se pode olvidar que os riscos virtuais emanam do simples fato de se conectar a uma rede (ainda que intranet ou offline), cabendo a cada qual a assunção de responsabilidades como forma de exercício de suas

[449] SILVA SÁNCHEZ, Jesús María. Politica criminal en la dogmática: algunas cuestiones sobre su contenido y límites. In: *Política criminal y nuevo derecho penal: Libro homenaje a Claus Roxin*. Barcelona: Bosch, pp. 17-30, 1997, pp. 22-23.
[450] Cf. Capítulo 4.4.
[451] Em razão da vulnerabilidade de diversos usuários, bem como tendo em vista a necessidade de efetiva implementação de educação digital, com incremento dos conhecimentos básicos do usuário médio virtual.

liberdades e, apenas assim, será viável a plena promoção do bem jurídico autodeterminação informática.

6.1.2. Teoria da imputação objetiva

Como aponta Roxin, a função evidente da imputação objetiva consiste em sinalizar quais relações causais são ações objetivamente típicas. Apenas em caso positivo passa-se a avaliar a tipicidade subjetiva, ou seja, a presença de dolo.[452] Visa a constatar, portanto, se determinada ação é de responsabilidade do autor ou se provém do acaso, de terceiros ou da própria vítima.

Trata-se, portanto, de uma teoria de imputação ou não do resultado ao agente, notando-se uma vinculação indissociável entre o desvalor da ação e do resultado.[453] Contudo, nem todas as ações provindas da manifestação de liberdade do agente são relevantes ao Direito Penal, mas apenas na hipótese de se constatar uma conexão normativa com o resultado. Essa conexão é delineada pela teoria do risco.

Disso se depreende uma tendência atual de deslocamento do núcleo da análise penal da tipicidade subjetiva para a objetiva, que se mostra relevante para a análise dos crimes informáticos. Devido a uma pluralidade de condutas potencialmente lesivas que surgem diariamente no ambiente virtual, um desenvolvimento mais refinado da tipicidade objetiva fornecerá ferramentas precisas para a imputação de práticas nocivas a bens jurídicos, mitigando-se o grau de subjetividade.

As contribuições da teoria da imputação objetiva em sede de crimes informáticos já foram aventadas por respeitáveis doutrinadores pátrios. Jesus e Milagre trazem hipóteses de sua aplicação para diminuição de um risco, como um autor que invade dispositivo informático para evitar um ataque cibernético em andamento, ou mesmo deleta dados de terceiros para prevenir sua obtenção indevida por *crackers*.[454]

Sydow aponta para o papel protagonista a ser adotado pelos usuários, e não de mero coadjuvante, afastando-se o paternalismo penal em razão de sua autocolocação em risco. Aponta, com isso, para a imprescindibilidade de assunção de obrigações imediatas pelo usuário.[455]

---

[452] ROXIN, Claus. *Politica Criminal y estrutura del delito.* Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992, p. 363.
[453] Ibidem, p. 365.
[454] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016, p. 159.
[455] BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013, pp. 697-698.

Crespo,[456] a seu turno, suscita a relevância da educação dos usuários como critério relevante para a exclusão ou mitigação da responsabilidade penal em razão dos riscos inerentes desse ambiente.

De fato, o ambiente informático é pautado pela noção de risco: pelo acrônimo IVI, apontado pela teoria das atividades rotineiras,[457] verifica-se que basta ao usuário ativar um dispositivo informativo para se tornar uma vítima em potencial. Assim como outras atividades cotidianas, como o tráfego de veículos, o manejo dos riscos torna-se uma constante, sendo essencial delinear a conexão normativa entre os riscos proibidos gerados pelo autor e o resultado lesivo a bens jurídicos próprios ou impróprios do usuário.

Trata-se, com isso, de selecionar quais condutas no ambiente virtual transpassam a produção de riscos permitidos ou penalmente tolerados normativamente, bem como verificar sua efetiva manifestação no resultado. Nesse estudo, o alcance do tipo merece especial atenção em razão da relevância da navegação diligente dos usuários como modo de prevenção delitiva, sendo apto a se afastar ou mitigar o nexo normativo de imputação penal em determinadas hipóteses.

6.1.2.1. Proibição de regresso

A vinculação entre as ciências naturais e o direito continua em vigor, de modo que não se pode renunciar a seu suporte fático, independentemente da teria adotada. Em decorrência disso, utiliza-se a teoria da equivalência das condições para a determinação da causalidade de uma conduta na análise penal.[458] Toda ação será causa se não puder ser suprimida sem que o resultado se elida, donde provém sua denominação de *sine qua non*. São condições iguais e equivalentes uma vez que não é possível determinar qual tem primazia sobre a outra.[459]

Contudo, essa relação causal muitas vezes é insuficiente para se imputar uma ação ao autor. Há ações que, embora causais, devem ser vistas como irrelevantes ao Direito Penal. Uma das críticas atinentes à teoria consiste na limitação de sua eficácia a situações em que o nexo causal é facilmente subsumível.[460] Destarte, a fórmula seria supérflua porquanto tautológica.[461]

---

[456] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 105.
[457] Cf. Capítulo 4.3. (Novas propostas criminológicas aos crimes informáticos).
[458] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, p. 347.
[459]JESCHECK, Hans-Heinrich**.** *Tratado de DerechoPenal: parte general*. Barcelona: Bosch, 1981, p. 251.
[460] OTTO, Harro. *Grundkurs Strafrecht: Allgemeine Strafrechtslehre*, Berlin: De Gruyter, 2004, pp. 58-59.
[461] A supressão mental de uma condição apenas pode ocorrer se de antemão há ciência acerca de sua causalidade. Nesse esteio, o conceito que há de ser definido aparece oculto em sua definição, o que resulta no postulado: "toda condição é causal se for causal". (JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación.* Madrid: M. Pons, 1997, p. 227).

Ademais, a teoria da equivalência das condições, uma vez baseada em leis empíricas naturais, acarreta um retrocesso causal infinito, de modo que inclusive os ascendentes do autor são vistos como causa de sua ação.[462]

A impropriedade da singela aplicação dessa teoria torna-se patente na sociedade de risco atual, em que o simples emprego nexo de causalidade natural levaria a resultados inadmissíveis. Quanto aos crimes informáticos, se cogitaria da responsabilização de toda a rede de *botnets*, computadores zumbis controlados a distância, porquanto se cada usuário não tivesse acionado seu dispositivo, o resultado danoso de *Denial of Service* não teria ocorrido. Ainda, o fluxo da rede trafega por diversos dispositivos informáticos ao redor do globo, o que levaria a uma responsabilização de cada usuário responsável pelo provedor em que o *malware* trafegar até encontrar seu alvo. Para evitar essas lacunas da teoria, é imprescindível selecionar criteriosamente causas relevantes sob o ponto de vista jurídico-penal para uma posterior valoração.

A partir da teoria de proibição de regresso, inspirada nas teorias de adequação social[463] e da relevância,[464] uma ação interventora, ainda que imprudente, de terceiro sobre um curso causal doloso não é relevante ao Direito Penal, porquanto a participação requer a presença de liame subjetivo em todos os agentes envolvidos na consecução do tipo penal.[465]

Com relação à criminalidade informática, a proibição de regresso é apta a limitar a responsabilidade penal de *cracker* em observância ao princípioo da culpabilidade. Toma-se por exemplo a prática do delito de invasão de dispositivo informático, por meio de *worms*, em que o dispositivo informático da vítima reenvia e-mails a todos seus contatos, sendo que alguns

---

[462] JESCHECK, Hans-Heinrich**.** *Tratado de DerechoPenal: parte general*. Barcelona: Bosch, 1981, pp. 256-257.

[463] Por meio dessa teoria, postula-se o requisito de probabilidade de que a ação realizada pelo autor proporcione o resultado. Funda-se na ideia de que apenas se poderá constatar responsabilidade jurídico-penal quando se tratar de uma ação que favoreça a produção do resultado, o que implica a exclusão de nexos causais anormais. (JESCHECK, Hans-Heinrich. *Op. cit*, p. 257). A teoria da adequação permite um juízo estatístico de resultados com base em experiências usuais, sem levar em conta as peculiaridades causais de cada caso, de modo a não possibilitar aferir a relevância normativa destas (JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación.* Madrid: M. Pons, 1997, p. 241). Portanto, essa teoria permite apenas a exclusão dos cursos evidentemente atípicos – que são a minoria -, sendo insuficiente como uma teoria conglobada da imputação objetiva.

[464] Segundo essa teoria, a responsabilidade jurídico-penal deve ser definida de acordo com as circunstâncias do caso concreto, visando-se a delimitar a amplitude da tipicidade ocasionada pelo causalismo e pela teoria da adequação. Entendem-se como causais apenas ações relevantes ao fim de proteção da norma penal. (RENGIER, Rudolf.*Strafrecht: Allgemeiner Teil*. 7. ed. Munique: Beck, 2012, p. 76). Trata-se de uma teoria precursora da atual imputação objetiva, porém sem critérios bem delimitados que viabilizassem sua aplicação. Ambas as teorias permitem a exclusão de cursos causais manifestamente descabidos. Assim, em sede de delitos informáticos, viabilizam o afastamento da responsabilidade de provedores que simplesmente conduzam fluxo informacional, como aqueles efetuados via TOR. No entanto, não permitem maior concreção de seus critérios.

[465] CAMARGO, Antonio Luís Chaves. *Imputação objetiva e Direito Penal.* São Paulo: Cultural Paulista, 2002, p. 151. Torna-se evidente a insuficiência da *conditio sinequa non* na resolução de casos desse teor, porque, ainda que presente a relação causal, deve-se excluir do âmbito penal o agente que não age de modo doloso.

conhecidos efetivamente efetuam depósitos ou fornecem dados pessoais aos golpistas. O computador infectado torna-se um "dispositivo zumbi", parte de uma botnet, que pode ser utilizada para efetuar novos ataques e na prática de outros delitos. Contudo, o usuário desse dispositivo infectado, ainda que tenha sofrido a invasão mediante negligência, não poderá ser responsabilizado pelos danos causados por seu dipositivo infectado. Ainda, se o *cracker A* promove a invasão de um dispositivo, tornando-o vulnerável em razão da criação de um *backdoor*, não será responsabilizado pela subtração de dados e furto promovida pelo *cracker B*.

A partir do desenvolvimento das teorias da adequação e da relevância,[466] fez-se possível delinear a teoria da imputação objetiva, a qual acresce critérios mais sólidos: uma conduta humana será imputável objetivamente se criou uma situação de risco juridicamente desaprovada, cujo perigo se materializou no resultado e se encontrava dentro do alcance do tipo penal.

6.1.2.2. Incremento do risco

Exclui-se a imputação objetiva quando não se constata a produção de um risco proibido. Não se pode considerar como típica uma atividade não perigosa, como convencer alguém a viajar de avião,[467] ou quando o perigo já é inerente à atividade, de modo que a atuação do agente não maximiza o risco.[468] Destarte, o risco será socialmente permitido se disser respeito a fatos irrenunciáveis dentro da vida em sociedade: são comportamentos inerentes ao cotidiano. Esse raciocínio também se aplica a ações perigosas dotadas de utilidade social.[469] Nesses casos, cria-se um risco relevante, contudo expressamente autorizado dentro da sociedade de risco. O principal exemplo consiste no tráfego automobilístico regulamentar.

É evidente a existência de riscos, ainda que mediante a observância das regras de trânsito, porém há interesses coletivos preponderantes reconhecidos pelo ordenamento. Em

[466] A teoria da imputação objetiva também se mune da análise de cursos causas hipotéticos efetuadas pelas teorias precursoras. Os cursos causais hipotéticos consistem na inevitabilidade de geração do resultado, ainda que ausente conduta do autor naquele caso cocnreto, porque outro substituto proporcionaria o mesmo resultado. Porém, a teoria da imputação objetiva não pode ser aplicada para excluir a responsabilidade do sujeito pelo fato de outro estar disposto a infringir a norma. Na seara virtual, ainda que um dispositivo informático esteja infectado por mais de um malware que vise a captar dados, ao *cracker* que primeiro invadir o dispositivo deverá ser imputada a prática prevista no artigo 154-A, do Código Penal, ainda que outro malware posteriormente efetuasse a invasão.
[467] JESCHECK, Hans-Heinrich, WEIGEND, Thomas. *Lehrbuch des Strafrechts, AllgemeinerTeil*. 2. ed. Berlin: Duncker & Hublot, 1996, p. 287.
[468] CAMARGO, Antonio Luís Chaves. *Imputação objetiva e Direito Penal.* São Paulo: Cultural Paulista, 2002, p. 73.
[469] Ibidem, p. 110.

verdade, os riscos juridicamente permitidos consistem em uma autorização prévia e absoluta do ordenamento, ainda que seja utilizada para fins juridicamente reprováveis.[470]

Assim, no ambiente informático, a mera solicitação a alguém para que acesse determinado website não poderá importar em responsabilização penal. Referido panorama poderá ser diferente caso se trate da *darkweb*, em que se requer conhecimentos informáticos de elevado grau para que não haja uma imediata contaminação do dispositivo informático. Nessas hipóteses, é necessário que o usuário seja informado acerca dos riscos, sob pena de aquele que o convenceu ao acesso adquira posição de garantidor. A análise do incremento de risco consiste, nesse sentido, em uma avaliação *ex ante* para se constatar ou não um perigo ao bem jurídico.

Segundo Roxin, outro critério de não imputação do fato ao agente consiste na diminuição do risco causada pela ação.[471] Nesses casos, ainda que se constate um dano ao bem jurídico em questão, a ação do sujeito ocasionou um resultado mais favorável ao mesmo, de modo a corroborar a finalidade do Direito Penal de proteção dos bens jurídicos. Perfaz-se uma análise objetivo-posterior de conduta, levando-se em conta os conhecimentos específicos do agente.

Pode-se citar aqui a contratação de empresas especializadas em segurança informática, as quais frequenemente tentarão invadir dispositivos informáticos em busca de debilidades rastreáveis pelos *crackers*. Nessa hipótese, ainda que haja acesso a dados sigilosos, trata-se de conduta redutora de riscos ao bem jurídico tutelado e, portanto, atípica. Isso se verificará ainda que os meios empregados excedam aqueles contratualmente pactuados. Do mesmo modo, caso um agente remova ou destrua dados sigilosos do dispositivo a fim de evitar sua obtenção por *crackers* autores de um ataque em andamento.

6.1.2.3. Realização do risco no resultado

Deve-se ressaltar que o risco, ainda que proibido, será juridicamente relevante apenas caso se manifeste no resultado.[472] Desta forma, se uma pessoa morre de infarto após um

---

[470] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, pp. 371-372. Não se contesta o fato de ser irrelevante o juízo subjetivo do autor para realizar a conduta. Trata-se, de uma aceitação *ex ante* da conduta do agente, manifestando-se tal ação como aceitável em sociedade. Portanto, causar um acidente de trânsito mediante a observância de todas as regras não implica uma configuração da tipicidade objetiva se o agente realiza outra conduta típica por meio do tráfego. Por exemplo, ao raptar uma pessoa, o autor responderá apenas por sequestro se o acidente de trânsito causado não proveio de um desrespeito a regras de trânsito.

[471] Note-se que é aplicada a teoria da equivalência das condições de modo prévio, o que demonstra a impossibilidade de sua exclusiva aplicação para a solução desses problemas.

[472] Em sua inicial concepção da teoria da imputação objetiva, à parte da manifestação do risco no resultado, Roxin traçava a categoria denominada "fim de proteção da norma". Segundo seu entendimento, as normas jurídicas apresentam um fim de limitação de risco e, portanto, um fim de proteção específico. Haveria casos em que o

acidente ocasionado de forma imprudente por um sujeito, não é admissível imputar-lhe o resultado porque o incremento do risco não é relevante para a morte.[473]

Um comportamento não permitido adicionado da causalidade nem sempre acarretará um comportamento proibido consumado. Consequentemente, a análise acerca da realização do risco jamais pode ser feita *a priori*, porquanto esse risco pode não estar presente, o que afasta a imputação do resultado.[474] De fato, se o resultado provindo da criação do risco consistir em mera casualidade, não haverá imputação do tipo objetivo. Nota-se uma imprevisibilidade do resultado, o que interrompe a relevância causal para o Direito Penal.[475]

Na seara informática, cogita-se da instalação subreptícia de *keyloggers* para obter senhas do usuário. Caso sua atividade em nada prejudique a atuação de um antivírus, posterior invasão do dispositivo da vítima por outro agente, com a obtenção imediata das mesmas senhas não poderá ser imputada àquele que instalou o *keylogger*.

Ademais, deve-se excluir a imputação de casos em que o incremento do risco proibido se manifeste posteriormente no resultado de modo imprevisível. Por exemplo, o motorista que dirige acima da velocidade permitida em um determinado trecho da pista posteriormente atropela uma pessoa já em velocidade normal e seguindo todas as regras de diligência. Nota-se, evidentemente, uma causalidade, porquanto se não tivesse dirigido acima da velocidade permitida não estaria no mesmo local naquele instante e, portanto, não teria atropelado a

---

incremento do risco não se encontra no âmbito de proteção da norma, de modo que sua finalidade de tutela exclui a imputação do resultado. (CAMARGO, Antonio Luís Chaves. *Imputação objetiva e Direito Penal*. São Paulo: Cultural Paulista, 2002, p. 79). Assim, o fim de proteção da norma seria distinto da manifestação do risco no resultado porque este consiste em um juízo de adequação ou previsibilidade do nexo causal. Contudo, ainda que o risco incrementado se realize no resultado, não haveria sua imputação se não era exigível ao agente evitar essa consequência específica, uma vez que não se tratava do fim de proteção da norma, mas apenas de um dever de cuidado. O fim de proteção da norma deveria se referir diretamente à tutela do bem jurídico (específico, inclusive de cada titular) do tipo penal em questão. (ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, p. 374-375). Posteriormente, Roxin reconhece que o fim de proteção da norma deve ser inserido na segunda categoria da imputação objetiva (manifestação do risco no resultado). Para o autor, refere-se apenas e tão somente ao fim de proteção da norma de cuidado que delimita o risco permitido, e não ao tipo penal em si. Com isso, traça uma distinção com relação ao alcance do tipo: este conceito configura uma vertente autônoma, posto que atinente à norma penal, com vistas a excluir de sua abrangência determinados comportamentos (notadamente, autocolocação em risco, heterocolocação em risco consentida e atribuição do âmbito de responsabilidade alheio). (ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, pp. 337-338). Dessa forma, atualmente, o fim de proteção da norma deve ser compreendido como hipótese de não realização do risco proibido no resultado, por excluir a imputação entre o risco gerado e o resultado, por ser considerado mero fruto do acaso. Na hipótese de delitos informáticos, se o agente invadir dispositivo para obter dados, porém, por se tratar de equipamento extremamente antigo, este for inutilizadopor sobrecarga previamente ao acesso às informações, não se deve imputar ao agente o delito de dano, porquanto não abarcado pelo âmbito de proteção da norma, de modo que o risco criado (invasão do dispositivo) não se manifestou normativamente no resultado (dano do *hardware*).

[473] CAMARGO, Antonio Luís Chaves. *Imputação objetiva e Direito Penal*. São Paulo: Cultural Paulista, 2002, pp. 78-79.

[474] Ibidem, p. 144.

[475] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, pp. 373-374.

pessoa.[476] Trata-se, em verdade, de um risco permitido, uma vez que o risco proibido não é controlável por interrupções temporais alheias à esfera do agente.

No ambiente informático, a instalação de *spywares* e *keyloggers* pode ser utilizada para obtenção de dados específicos sobre os usuários consumidores, a fim de alimentar um banco de dados para potenciais vendas virtuais. Ocorre que, caso esses dados sejam indevidamente obtidos por terceiros, sem qualquer liame subjetivo prévio, como na prática de estelionato ou acesso a contas bancárias, não haverá imputação desses ulteriores delitos ao agente que inicialmente obteve os dados.[477]

Todavia, há uma imputação do resultado ao agente se sua conduta anterior aumentou o perigo do curso causal posterior de forma previsível e juridicamente relevante, caso o risco tenha influenciado e se manifestado na materialidade da ação.[478] Assim, apesar de haver certo desvio causal em relação ao planejado pelo agente, este é minimamente previsível e até esperado. Por exemplo, ao se atirar uma pessoa em um rio para se afogar, esta pode morrer devido a um traumatismo craniano causado pela queda. Ou mesmo, na seara informática, caso o agente vise a invadir o dispositivo para ler dados específicos, porém o *malware* instalado subtrai todas as informações.

6.1.2.4. Alcance do tipo

Para Roxin, o alcance do tipo consiste no terceiro nível de análise da imputação objetiva. Não se confunde com o conceito anterior (manifestação do risco no resultado) por dizer respeito ao fim de proteção da norma inscrita no tipo penal em si, o qual não compreende o resultado ocorrido à luz de postulados político-criminais.[479] Diferentemente de outros adeptos da teoria

---

[476] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, p. 376.

[477] Por outro lado, uma consequência posterior de um dano pode ser imputada ao agente se o nexo temporal não impede uma manifestação previsível do risco no resultado. Há consequências tardias com que não incumbe à vítima lidar, mas ao agente. Na seara informática, pode-se pensar em uma invasão a dispositivo informático que destrua o mecanismo de segurança, vindo o agente a extrair dados apenas meses depois em razão da falta de proteção do sistema.

[478] RENGIER, Rudolf.*Strafrecht: Allgemeiner Teil*. 7. ed. Munique: Beck, 2012, pp. 91-92. O curso causal também é considerado imprevisível se a vítima possui uma estrutura física distinta e imprevista pelo agente que aumente sua fragilidade à determinada ação. Portanto, se um hemofílico vier a falecer por perda de sangue após uma facada no braço, este resultado não pode ser imputado ao agente se este não tinha ciência dessa circunstância. Contudo, Jescheck e Weigend afirmam que, como o âmbito de proteção da normal deve incluir todas as pessoas, o resultado será imputado ao agente mesmo se provier de constituições físicas anormais. Indaga-se apenas a previsibilidade do resultado. (JESCHECK, Hans-Heinrich; WEIGEND, Ewa. *Tratado de derecho penal: parte general*. Granada: Comares, 2003, p. 209).

[479] ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, p. 352.

imputação objetiva, que defendem apenas dois planos de análise,[480] Roxin inclui no alcance do tipo os elementos de autocolocação da vítima, heterocolocação em risco consentida e atribuição do âmbito de responsabilidade alheio.

No tocante à autocolocação da vítima em risco, essa teoria surgiu a com vistas à aplicação em três casos concretos: a) hipóteses de consumo conjunto de drogas injetáveis, vindo um deles a adquirir AIDS; b) participação em suicídio; c) transmissão de AIDS em relações sexuais, diante do assentimento do parceiro, ciente da condição que acomete o autor. [481]

Para Roxin, a autocolocação em risco pode ser traduzida na contribuição de alguém para que a vítima pratique alguma ação perigosa. Sob a ótica do direito alemão, há um sólido e simples raciocínio: dado que a participação em suicídio, referente ao bem jurídico de maior valor (vida), é atípica, tampouco merece punição a simples contribuição a um risco proibido, efetuando-se um argumento *a maiorum ad minus.*[482]

Em um raciocínio expansível ao ordenamento brasileiro, trata-se de uma incorporação à teoria da imputação objetiva do princípio da autorresponsabilidade: visto que a vítima possui completa ciência do risco e o controla, não há razão para incidência do direito penal. Por outro lado, se o agente contribuidor possui maior ciência acerca dos riscos do que a vítima, o resultado lhe será imputável, por não incidir o princípio da autorresponsabilidade.[483]

Conforme discorre Feijóo Sanchez, a autorresponsabilidade converte-se em um filtro no âmbito do alcance do tipo, dizendo respeito a hipóteses em que, apesar de a vítima não ter voluntariamente anuído com o resultado – excluindo-se hipóteses de acordo e consentimento – , este é fruto de uma decisão livre e responsável de seu titular.[484]

A relevância da autocolocação em risco consiste em fornecer solução mais adequada a problemas originalmente inseridos na proibição de regresso. Isso porque não se trata de problema de causalidade, mas efetivamente de imputação no caso concreto, visto que nem toda intervenção de terceiro será apta a interroper o nexo da imputação.[485]

A autocolocação em risco é de primordial importância para os crimes informáticos, sendo tratada com destaque no Capítulo 6.5. A partir dos parâmetros delineados por novas

---

[480] Outros autores, como Cancio Meliá, optam por tratar esses institutos no plano de criação de riscos, em uma categoria que abranja tanto os riscos derivados da norma delimitadora de risco permitido, como também do tipo penal em si.
[481] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p.103.
[482] ROXIN, Claus; GRECO, Luís. *Op. cit.*, p. 354.
[483] Ibidem, p. 360.
[484] FEIJÓO SÁNCHEZ, Bernardo José. Actuación de la víctima e imputación objetiva: comentario a la STS del 17 de septiembre de 1999. *Revista de Derecho Penal y Criminología*, n. 5, p. 265–333, 2000, p. 326.
[485] ROXIN, Claus; GRECO, Luís. *Op. cit.*, p. 366.

teorias criminológicas, deve-se refletir acerca de condutas dotadas de elevado grau de negligência, como a não instalação de *antimalware* ou atualização, mesmo após diversos alertas do dispositivo, uso de senhas fracas, realização de compras de produtos por preços inferiores ao de mercado em sites suspeitos, entre outros. A seu turno, nem toda postura imprudente ou negligente do usuário deve ser apta a interromper o nexo de imputação, perquirindo-se a posição assumida pelo agente e pela vítima no caso concreto, bem como as condições subjetivas de cada usuário, à luz dos perfis vitimológicos informáticos delineados no Capítulo 4.4. (Proposta de classificação das vítimas informáticas).

Avançando na classificação de Roxin, a heterocolocação em risco consentida diz respeito a hipóteses em que o indivíduo, ciente do risco em que incorre, deixa-se colocar em perigo por terceiro.[486] Hipóteses mais frequentes se referem a atividades no trânsito, como indivíduo que concorda em receber uma carona de uma pessoa embriagada ou para participar de um "racha". [487]

A relevância da heterolococação em risco em sede de delitos informáticos surge, a título exemplificativo, ao ceder a terceiros o *login* ou acesso ao dispositivo, estando ambos cientes de possíveis falhas de segurança (como ausência de *frewall*) que acometem o equipamento. Tendo em vista que o uso de dispositivo informático alheio é prática corriqueira em empresas e nos lares, a heterocolocação em risco consentida obtém ampla guarida no ambiente virtual. Pode-se citar ainda o acesso a *links* e *websites*, aquisição de produtos ou transferências financeiras por meio de *Internet Banking* a rogo de terceiro, desde que ambos tenham ciência dos riscos que cercam aquela conduta.

Por fim, a terceira hipótese inserida no alcance do tipo, o âmbito de responsabilidade alheia, guarda correlação com situações em que o terceiro, por força de especial posição na situação concreta ou em decorrência de sua profissão ou ofício, tem obrigação de vigilância e salvamento da vítima.[488]

---

[486] A distinção entre autocolocação em risco e heterocolocação consentida, embora seja viável ao considerar quem causa o risco concretamente (no primeiro caso, a vítima, no segundo, o autor), essa classificação não se mostra útil, posto que os pressupostos e a solução jurídicos são rigorosamente idênticos, quais sejam: vítima capaz e espontaneamente se submete a um risco do qual está ciente, o que resulta na exclusão do tipo penal. (GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 119).

[487] Tradicionalmente nessas hipóteses utiliza-se a figura do consentimento para se afastar a responsabilidade do motorista. Ocorre que essa não se revela uma solução adequada, afinal, a vítima apenas anui com a conduta por acreditar na inocorrência do resultado lesivo. (ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, p. 368). Assim, a exclusão pela via da imputação objetiva mostra-se mais adequada nas hipóteses em que a vítima possui ciência dos riscos e com eles concorda, porém não espera a incidência do dano concreto.

[488] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 120.

Nesse esteio, os bombeiros, policiais e salva-vidas apresentam responsabilidade de se colocar em risco que outras pessoas não possuem. Desse fato decorre que os riscos profissionais são voluntários e previamente aceitos. Ademais, se houvesse a possibilidade de punir o agente pela morte eventual de profissionais, não se recorreriaaos bombeiros para cessar o incêndio, o que acarreta a desnecessidade de imputação por fins político-criminais.[489] Sob a perspectiva dos delitos informáticos, é digna de menção a infiltração virtual de agentes na *darkweb*, mormente em hipóteses de investigação de infrações penais ao Estatuto da Criança e do Adolescente, recaindo-se maior deve ser exposição do dispositivo e até mesmo dispêndios financeiros.

6.2. Contribuições de outras teorias funcionalistas

O funcionalismo penal encontra-se em constante construção e alteração. Nesse contexto, muito embora a proposta de Roxin receba maior adesão doutrinária, outras proposts funcionalistas mostram-se profícuas e são aptas a trazer contribuições relevantes à seara penal, inclusive no que tange ao estudo dos delitos informáticos. Isso porque trazem outras perspectivas para a estrutura da teoria da imputação objetiva, bem como nova ótica à questão do envolvimento da vítima, o que, de qualquer modo, ocupa aspecto central.

Nos subcapítulos seguintes, serão abordadas as teorias funcionalistas de Günther Jakobs e Cancio Meliá.

6.2.1. Funcionalismo sistêmico de Günther Jakobs

Jakobs é um dos principais representantes do denominado funcionalismo sistêmico. Assim como os demais funcionalistas, entende inviável uma fundamentação dogmática sob a perspectiva meramente ontológica, visto que não se está a falar de estruturas lógico-objetivas preexistentes.

Para Jakobs, a teoria do delito deve se orientar para os fins do direito penal, não vistos como a proteção de bens jurídicos, mas sim sedimentados na vigência da norma, de modo a reafirmar a prevalência do direito.[490] Sua teoria apresenta um lastro distante em Hegel, o qual

[489] ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997, pp. 399-400.
[490] ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, p. 125.

defende a sanção penal como a negação à negativa de vigência da norma, consubstanciada pelo delito.

Contudo, Jakobs dá um passo além, com base na teoria de Luhmann: a partir da teoria dos sistemas, entende que o direito consiste em uma estrutura que facilita a orientação social mediante redução de sua complexidade, o que viabiliza a generalização de expectativas. Logo, para Jakobs exsurge um novo conceito de bem jurídico, entendido como expectativas fundamentais para conservação da identidade social.[491]

As normas penais regulam o comportamento humano com a finalidade de assegurar expectativas sociais e assim possibilitar a vida social. Assim, devem ser compreendidas como "expectativas de comportamento estabilizadas contrafaticamente."[492]

Contemplando-se o funcionalismo sistêmico sob a ótica dos crimes informáticos, volta-se a uma regulação de expectativas de comportamento dos usuários quando de sua navegação. Privilegia-se, assim, a vigência de normas reguladoras no ambiente virtual, relegando-se para segundo plano a tutela ao bem jurídico autodeterminação informática. Muito embora a delineação de expectativas nesse ambiente não necessariamente conduza a um cerceamento das liberdades individuais, não está descartado que uma regulamentação de expectativas possa culminar com um ambiente informático policialesco e de vigilância, tolhendo-se as liberdades individuais. Contudo, vislumbrando-se o funcionalismo sistêmico sob a ótica constitucional do Estado Democrático de Direito, suas contribuições podem ser profícuas para se delimitar quais os comportamentos esperados socialmente dos usuários, bem como viabilizar a defraudação de determinadas expectativas informáticas em prol de maiores liberdades nesse novo ambiente.

Avançando na teoria funcionalista sistêmica, Jakobs aponta que essa configuração do risco permitido ocorre justamente porque a principal função do Direito Penal consiste em assegurar expectativas, não necessariamente conservar e maximizar os bens jurídicos. Destarte, uma ação que cause danos a bens jurídicos, mas seja socialmente aceita não levará a relevância penal.[493] Caso haja observância a um feixe de expectativas (papel social) que recaem sobre o sujeito, não há que se falar de violação de norma e, portanto, do direito penal. Nesse esteio, a construção de Jakobs se aproxima dogmaticamente à função de garante de crimes omissivos

---

[491] LYNETT, Eduardo Montealegre. Introdução à obra de Günther Jakobs. In: CALLEGARI, André Luís et al. *Direito penal e funcionalismo.* Trad. André Luís Callegari. Porto Alegre: Livraria do Advogado, 2005, p. 13-14.
[492] ROXIN, Claus; GRECO, Luís. *Op. cit.*, pp. 125-127.
[493] JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación.* Madrid: M. Pons, 1997, p. 244.

impróprios: trata-se de evitar riscos normativamente vedados, sendo irrelevante se mediante ação ou omissão.[494]

Assim, o primeiro nível da análise de Jakobs consiste em aferir a posição de garantia do sujeito, quer em razão de seu papel social, quer pela prévia criação de um risco proibido.[495] Verifica-se, com isso, que Jakobs busca superar o dualismo entre o conceito de ação e omissão, transformando qualquer conduta penalmente relevante em violação a um dever. Disso decorre que as normas não são meras proibições, mas verdadeiros imperativos dirigidos às pessoas acerca da organização de seu corpo, patrimônio e direitos. Essa obrigação consiste em "manter o próprio âmbito da livre organização numa situação inócua para os demais," compreendida dentro daquilo aceito socialmente.[496]

No ambiente informático, os pais adquirem posição de garantidores frente a seus filhos, sendo responsáveis por evitar a exposição a riscos usualmente conhecidos, de modo que lhes incumbe a adoção de cautelas e supervisão de crianças e adolescentes. Ademais, idosos costumam ter alguém de sua confiança para auxílio no ambiente virtual – filhos, netos –, que são aptos a assumir essa posição de garante a depender do caso concreto. Deve-se ter cautela, contudo, para evitar excessiva responsabilização penal desses garantidores, de modo que a regulamentação de suas obrigações deve provir prioritariamente das esferas cíveis e administrativa, à luz dos princípios penais da subsidiariedade e fragmentariedade.

No bojo da teoria da imputação objetiva, verificada a posição de garantia, Jakobs cria quatro principais níveis de análise de criação de risco juridicamente desaprovado: princípio da confiança (nem tudo incumbe a todos, outros devem cumprir seu papel), risco permitido (não viola expectativas), comportamento socialmente neutro (veda regresso, mesmo se usem seu comportamento para fins criminosos, como vender arma), risco no âmbito de competência da vítima (consentimento excludente de tipicidade, autocolocação em risco).

Um dos principais pressupostos para o risco permitido consiste no princípio da confiança. Segundo este, embora outras pessoas cometam erros, é aceitável e aconselhável confiar em um comportamento do próximo conforme o direito. Dessa forma, esse princípio propicia a proibição de regresso, na medida em que outrem, geralmente, não será responsabilizado por um erro de terceiro.[497]

---

[494] ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, p. 125.
[495] LYNETT, Eduardo Montealegre. Introdução à obra de Günther Jakobs. In: CALLEGARI, André Luís et al. *Direito penal e funcionalismo.* Trad. André Luís Callegari. Porto Alegre: Livraria do Advogado, 2005, p. 24.
[496] JAKOBS, Günther. *A imputação penal da ação e da omissão*. Barueri: Editora Manole, 2003, p. 26.
[497] JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación*. Madrid: M. Pons, 1997, p. 253.

Dentro do risco permitido, segundo Jakobs, para viabilizar um rol de possibilidades distintas de condutas perante o contato social, é necessário aceitar algumas frustrações de expectativas, de tal forma que a aceitação do risco será tão maior quanto for ampla a liberdade de atuação do sujeito em cada caso concreto.[498] Realiza-se uma ponderação de interesses levando-se em conta a amplitude do risco, bem como sua utilidade e prejuízos para se definir se se trata de interesses penalmente tutelados. É justamente a hipótese de conformação dos delitos informáticos, em que se mostram necessárias a anuência e a tolerância de determinados resultados gravosos com vistas a preservar as liberdades individuais no ambiente virtual.

Por outro lado, há determinadas ações em que não se faz possível um juízo de utilidade, porquanto não se poderia contemplar sua ausência na sociedade. Trata-se de ações historicamente legitimadas, as quais são aceitas ainda que possam ser mais prejudiciais após um adequado sopesamento. Nesse sentido, entende-se o tráfico de veículos como uma ação socialmente adequada, cabendo ao direito apenas regulamentá-lo.[499] Atualmente, referido raciocínio passa a ser estendido ao ambiente informático, em que se torna inconcebível qualquer retrocesso de fluxo informacional, ainda que se mostre em certa medida prejudicial aos usuários: sua legitimação social é ampla na sociedade de rede atual, verificando-se sua irreversibilidade.

A prática de condutas socialmente neutras dentro do papel social desempenhado pelo sujeito consiste em outro mecanismo de aplicação da proibição de regresso. Para Jakobs, assim, são irrelevantes conhecimentos e capacidades especiais do autor, desde que este aja de acordo com aquilo socialmente requerido de seu papel social.[500]

Por fim, segundo Jakobs, condutas atribuídas ao âmbito de competência da vítima não geram um risco juridicamente desaprovado, porquanto não violam as expectativas sociais que recaem sobre o autor. Afinal, a teoria da imputação objetiva visa a determinar tarefas objetivas de incumbência de cada indivíduo. Frequentemente, contudo, a obrigação poderá recair sobre terceiras pessoas e, notadamente, sobre a própria vítima, com fundamento no princípio da autorresponsabilidade.[501]

Assim, a depender do papel social desempenhado pela vítima, pode ser-lhe incumbido o comportamento lesivo em seu âmbito de competência, de modo que a conduta não deverá ser

---

[498] JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación*. Madrid: M. Pons, 1997, p. 253.
[499] Ibidem, p. 244.
[500] ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, p. 127.
[501] JAKOBS, Günther. *A imputação penal da ação e da omissão*. Barueri: Editora Manole, p. 36.

atribuída ao autor. Destarte, a autocolocação da vítima em risco, bem como o consentimento quanto a bens jurídicos disponíveis voltados ao livre desenvolvimento de sua personalidade, para esse autor, são inseridos na primeira fase da imputação objetiva, afastando-se o instituto do alcance do tipo elencado por Roxin.[502]

A teoria dos papéis sociais do funcionalismo sistêmico permite traçar as responsabilidades incumbentes a cada usuário no ambiente virtual: quais comportamentos são socialmente esperados e quais informações devem ser fornecidas. A título exemplificativo, à luz do âmbito de competência decisório na seara informática, pode-se exigir o fornecimento de determinadas informações como pressuposto para o acesso regular ao computador, dados, ou aplicativos em dispositivos portáteis. Torna-se relevante, assim, compreender socialmente qual o grau de informação a ser fornecido ao usuário e quais as condutas diligentes devem ser por ele adotadas "de ofício".

Essa teoria também permite a mitigação das expectativas sociais que recaem sobre vítimas jovens e idosas, nos quais naturalmente repousam menores deveres de cautela em razão de sua condição. Do mesmo modo, não se imputa ao âmbito de competência da vítima tecnicamente ignorante os mesmos deveres previstos para o homem médio. Quanto ao ponto, coaduna-se a proposta de educação digital irrestrita da população, o que permitirá uniformizar os papéis sociais virtuais.

Essa abordagem sugerida na seara informática, apesar de aparentemente confluir com critérios político-criminais sugeridos por teorias criminológicas, não consiste em um caminho a ser forçosamente adotado por adeptos do funcionalismo sistêmico, considerando-se que a construção futura de expectativas sociais poderá inclusive predominar sobre os estudos vitimológicos. Ou seja: muito embora seja desejável e já se constate o surgimento de expectativas sociais mínimas no ambiente informático, o funcionalismo sistêmico traz critérios excessivamente fluidos para embasar o âmbito de competência da vítima no ambiente virtual.

Na segunda fase de análise da imputação objetiva, qual seja, a realização do risco juridicamente desaprovado no resultado, Jakobs propõe o isolamento do risco não permitido: se este, por si, explicar o resultado, não haverá imputação.[503] Para esse raciocínio, Jakobs defende que o autor deve ser responsável pelo incremento do risco proibido que acarrete o

---

[502] JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación*. Madrid: M. Pons, 1997, pp. 293-295. De particular relevância são as denominadas ações a próprio risco, que serão analisadas em Capítulo próprio.

[503] ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002, p. 128.

resultado por uma ameaça *ex ante*. Os delitos de resultado podem ser vistos, destarte, como delitos de perigo condicionados pelo resultado.[504]

Como se vê, Jakobs propõe soluções para a imputação objetiva com notável estrutura e coerência internas, ao sempre considerar o papel social desempenhado pelo sujeito ativo. Ocorre que sua teoria, lastreada no funcionalismo sistêmico, estabelece uma abdicação radical da teoria dos bens jurídicos para criar um modelo autorreferencial, com base na teoria de Luhmann, em última análise, tautológico.

Isso porque, ao postular o reforço normativo como única finalidade do direito penal, mostra-se resistente à exsurgência de novos valores sociais e alheio à dinamicidade com que condutas antes tipificadas podem deixar de merecer tutela penal. Um alinhamento político-criminal, vinculado à teoria do bem jurídico conforme proposto por Roxin, fornece as ferramentas necessárias para a devida consideração dos valores sociais, sem renunciar à importância de certas expecativas para a vida em sociedade. Mostra-se, dessa forma, aquele mais adequado para a abordagem dos delitos informáticos.

De qualquer modo, deve-se reconhecer que não se trata de um sistema integralmente fechado, porquanto deve se ater à realidade social – donde se extraem as expectativas e papéis sociais-, a qual, por si, amolda influxos criminológicos. Por essa razão, Jakobs também entende como aceitável a frustração de determinadas expectativas sociais, cuja manutenção implicaria excessiva limitação das liberdades individuais.

No ambiente virtual, esse raciocínio permite concluir pela defraudação de certas expectativas de tutela penal em hipóteses nas quais a proibição implicaria excessivo tolhimento da liberdade no exercício de atividades informáticas.[505]

---

[504] JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación*. Madrid: M. Pons, 1997, p. 285. Deve-se ter cautela na afirmação de que todas as infrações penais sejam essencialmente delitos de perigo dado seu potencial de fomentar a expansão penal, violando-se o princípio da subsidiariedade. Referida problemática recebe especiais contornos na sociedade de risco, em que já se verifica certa antecipação da tutela penal. Sob a ótica informática, crimes de perigo começam a ser elaborados pelo legislador penal, como o previsto no artigo 154-A, § 1º, do Código Penal.

[505] A isso agrega-se a perene contestação acerca da efetiva existência de bens jurídicos em certos crimes, a título exemplificativo, ante delitos de mera conduta e interesses difusos. Aliás, inclusive Claus Roxin passa a admitir a existência de determinados delitos desprovidos de bem jurídico concretamente tutelado, como a proteção de embriões, plantas e animais. (SILVEIRA, Renato de Mello Jorge. *Fundamentos da adequação social em direito penal*. São Paulo: Quartier Latin, 2010, p. 47). Assim, há valores sociais para os quais não se atribui imediatamente um bem jurídico digno de tutela, nos quais a teoria funcionalista sistêmica pode obter maior amparo. Nesse ponto, a teoria de Jakobs fornece uma explicação adequada, qual seja: muitas normas penais existem tão somente com fins de manutenção de expectativas socialmente vigentes. Do mesmo modo, não se pode ignorar a incorporação de certos elementos atinentes ao direito penal do inimigo na seara do combate à criminalidade organizada, sendo de rigor evitar-se uma visão maniqueísta acerca das concepções do autor.

6.2.1.1. Ações a próprio risco

A partir do desenvolvimento da concepção de papéis sociais, dos quais derivam âmbitos de organização próprios de cada indivíduo, Jakobs analisa a responsabilidade por consequências não desejadas de um contato social, quer de forma prevista, ou mesmo, não prevista por seu titular.

Segundo esse autor, uma ação de forma consciente ou inconscientemente descuidada com os próprios bens pode culminar com uma ação a próprio risco, eximindo de responsabilidade o causador da lesão. São hipóteses em que um terceiro cria, facilita ou favorece uma situação na qual a vítima, titular do bem jurídico, promove uma ação perigosa que lesiona ou põe em risco esse bem.[506]

Sob esse conceito, podem-se abarcar a autocolocação em risco, a heterocolocação em risco consentida, ações arriscadas de salvamento. No entanto, não se fala apenas de comportamentos imprudentes, mas também dolosos, sempre que haja consequências suficientemente intensas. Surge aqui um paralelismo com o consentimento, o qual não surge de aspecto piscológico, mas efetivamente normativo.[507]

Nesse contexto, adquire relevância o princípio da autorresponsabilidade também para a teoria de Jakobs. López Días, com base em Jakobs, traz os pressupostos para atribuição da ação de próprio risco à vítima. Primeiramente, a autora aponta para a necessidade de que a atividade permaneça no âmbito de organização conjunta do autor e da vítima, de modo que esta possua controle sobre o desenrolar da conduta (ou seja, possa se abster de continuá-la).[508] Como discorre Feijóo Sánchez, o critério decisivo para a incumbência do âmbito de organização da vítima consiste no "domínio sobre a decisão", de modo que somente quando o autor retira esse domínio não se torna possível imputar o resultado à vítima.[509]

Nessa hipótese, verificado o resultado, a vítima possui âmbito de organização preferencial, considerando que é um sujeito autorresponsável e, por conseguinte, autônomo para desenvolvimento de sua personalidade, o que implica também liberdade de exposição a risco e lesões de seus bens jurídicos. [510]

---

[506] LÓPEZ DÍAS, Claudia. Acciones a próprio riesgo. *Revista CENIPEC*, v. 25, n. 1, p. 115-174, 2006, pp. 120-121.
[507] JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación*. Madrid: M. Pons, 1997, pp. 304-306.
[508] LÓPEZ DÍAS, Claudia. *Op. cit.*, pp. 146-147.
[509] FEIJÓO SÁNCHEZ, Bernardo José. Actuación de la víctima e imputación objetiva: comentario a la STS del 17 de septiembre de 1999. *Revista de Derecho Penal y Criminología*, n. 5, p. 265–333, 2000, p. 311.
[510] LÓPEZ DÍAS, Claudia. *Op. cit.*, pp. 147-148.

No entanto, essa autorresponsabilidade da vítima deve ser aferida concretamente, de modo que ela possua habilidade para calcular o risco a que está sujeita, ou seja: o risco deve ser ao menos cognoscível. Por fim, o autor não pode ocupar uma posição de garante perante essa pessoa que se expõe a riscos. [511]

Como aponta Feijóo Sánchez, é notória a contribuição de Jakobs na normatização do conceito de autorresponsabilidade, que implicará uma autolesão atípica caso a vítima atue de forma dolosa, ou mesmo pouco diligente consigo mesma, afastando-se do papel social de proteção atribuído puramente ao autor.[512]

Como se vê, a teoria das ações a próprio risco retoma as noções vitimodogmáticas de autorresponsabilidade, bem como dialoga com a teoria do alcance do tipo de Roxin. À diferença deste, porém, Jakobs expande sua concepção para condutas dolosas. Entretanto, por se lastrear no funcionalismo sistêmico, a teoria pode carecer de critérios mais sólidos, posto que não recebe os influxos criminológicos e político-criminais da teoria funcionalista moderada.

A teoria de ações a próprio risco possui âmbito de estudo profícuo em sede de delitos informáticos, delimitando-se o âmbito de organização pertencente a cada usuário do ambiente virtual, o que repercutiria em deveres de diligência por cada qual durante a navegação. Ocorre que não postula um lastro necessário em critérios político-criminais, demaneira que as teorias criminológicas – situational crime prevention, routine activities theory, general theory of crime – não incidem de forma direta, mas apenas de forma mediata, à luz e na medida em que as expectativas sociais se alinhem. De qualquer modo, por ser dotada de certa porosidade e abertura à realidade social, são válidos os influxos da criminologia para a delimitação do âmbito de competência preferencial dos usuários.

6.2.2. Imputação à vítima de Cancio Meliá

Manuel Cancio-Meliá traz contribuições de suma importância para a teoria da imputação objetiva ao inserir aportes vitimodogmáticos em sua estrutura. Meliá refuta a aplicação indistinta do princípio vitimológico sem um *topos* definido na parte geral. Para o autor, fomentar-se-ia a insegurança jurídica, posto que ausente um critério como parâmetro de aplicação.

---

[511] LÓPEZ DÍAS, Claudia. Acciones a próprio riesgo. *Revista CENIPEC*, v. 25, n. 1, p. 115-174, 2006, pp. 151-153.

[512] FEIJÓO SÁNCHEZ, Bernardo José. Actuación de la víctima e imputación objetiva: comentario a la STS del 17 de septiembre de 1999. *Revista de Derecho Penal y Criminología*, n. 5, p. 265–333, 2000, p. 311.

Por essas razões, ao recorrer ao princípio da autorresponsabilidade, Meliá o vê como inserido na teoria da imputação objetiva, a reforçar a importância da contribuição na análise da criação de um risco proibido.

Em sua teoria, Roxin insere a importância da participação da vítima no terceiro nível da imputação objetiva (alcance do tipo), com enfoque na autocolocação em risco e na heterocolocação em risco consentida. Para Meliá, contudo, essa estruturação sistemática é equivocada, porquanto introduz em marco dogmático posterior à realização do risco no resultado um fator que pertence à constatação prévia de criação de risco proibido. Assim, trata-se de contrassenso reconhecer a realização do risco no resultado para, posteriormente, afastar-se a tipicidade da conduta.[513_514]

Com efeito, o autor reconhece que a vítima será um dos fatores determinantes para a delimitação do risco permitido, tendo em vista que as expectativas que sobre ela recaem torna-se um critério decisivo de ponderação.[515] Ao propor uma reformulação da imputação objetiva, Meliá denomina sua teoria de "imputação à vítima" ao suscitar que:

> Quando o titular de um bem jurídico ("vítima") empreende conjuntamente com outro ("autor") uma atividade que pode produzir uma lesão a esse bem jurídico, a atividade criadora do risco deve ser imputada ao âmbito de responsabilidade preferencial da vítima.[516]

Para sua configuração, Meliá estabelece três pressupostos essenciais e concomitantes: a) permanência da atividade no âmbito de organização conjunta; b) conduta autônoma da vítima, sem instrumentalização pelo autor; c) carência de dever de proteção específico do autor frente à vítima (posição de garante). Preenchidos esses requisitos, Meliá entende que a imputação do resultado recairá sobre o âmbito de responsabilidade da vítima, considerando-se atípica a conduta para o autor. [517]

Ao reconhecer o âmbito de organização conjunta entre autor e vítima, à luz do princípio da autorresponsabilidade, Meliá tem como indiferente a disposição psíquica do autor. Logo,

---

[513] Tradução livre do original: "Cuando el titular de un bien -jurídico ("víctima") emprende conjuntamente con otro ("autor") una actividad que puede producir una lesión de ese bien jurídico, la actividad generadora del riesgo debe ser imputada al ámbito de responsabilidad preferente de la víctima." (MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 497).

[514] MELIÁ, Manuel Cancio. *Op. cit.*, p. 498. Por outro lado, Meliá reconhece o mérito da classificação de Roxin: demonstra que a especificidade normativa da questão merece um tratamento diferenciado, que não pode ser abordado de forma genérica no âmbito de criação de risco proibido.

[515] Ibidem, p. 521.

[516] Ibidem, p. 463.

[517] Ibidem., pp. 463-465.

pouco importa se o autor age de modo imprudente ou se atua com dolo eventual, posto que o risco criado sobre o bem jurídico é criado conjuntamente por ambos, sendo certo que a decisão ulterior e o domínio sobre o risco assumido recaem sobre a vítima.[518]

No famigerado exemplo da vítima que mantém relações sexuais com o autor, ciente de que este é portador de vírus HIV, é irrelevante perquirir acerca de seu elemento subjetivo, posto que a atuação autônoma e consciente da vítima retira a esfera de responsabilidade do portador.[519]

Para além da categoria de imputação à vítima no primeiro nível de imputação objetiva, Meliá também reconhece a contribuição do sujeito passivo para a própria delimitação do conceito de risco proibido. Para o autor, a particular posição da vítima em relação a seus bens jurídicos e a valoração de sua interação com o autor são critérios relevantes para a apuração dos riscos desvalorados juridicamente.

Ao se delimitar o risco permitido, entendido como âmbito normal de interação em sociedade, deve-se considerar as expectativas das vítimas em potencial, justamente porque o exercício permitido dessa atividade depende da anuência – acordo ou consentimento – da vítima. Ao fim, cuida-se de *apurar em que medida a vítima está disposta a assumir riscos de forma razoável*, como jogadores de futebol eelutadores de boxe. Afinal, inclusive em atividades permitidas que pressupõem certo grau de lesão ao bem jurídico, traçam-se limites insuperáveis, em que se presume a dissonância da vítima com o resultado.[520] Por essa razão, em esportes marciais, são vedados golpes nas partes genitais e na região da laringe.

A imputação à vítima, para o autor, também exerce influência sobre o princípio da confiança. Afinal, recai sobre a vítima a expectativa de que atuará de modo determinado de acordo com as regras existentes. Dessa forma, reconhece Meliá que o princípio da confiança é também um mecanismo de delimitação de âmbitos de responsabilidade.[521]

Na esteira do alcance do tipo do funcionalismo moderado e das ações a próprio risco atinentes ao funcionalismo sistêmico, Meliá também reconhece a importância da atuação da vítima no que tange a seu âmbito de organização. Procede a uma correção à teoria funcionalista de Roxin, ao afastar a própria criação de risco proibido diante da imputação da conduta à vítima.

---

[518] MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal*. Tese de Doutorado. Universidad Autónoma de Madrid, 1997, p. 471.

[519] Esse raciocínio também se aplica ao consumo de entorpecentes, de modo que ao indivíduo fornecedor do produto (quer por ser traficante, quer para juntos consumirem) não se pode atribuir a morte do consumidor por overdose.

[520] MELIÁ, Manuel Cancio. *Op. cit.*, pp. 521-524.

[521] Ibidem, p. 533.

Por outro lado, a teoria de Meliá revela-se contida, visto que não delineada para delitos dolosos, apesar de sua idoneidade para explicá-los. Na sociedade de risco atual, da qual o ambiente informático é seu integrante, apesar de não desejar a efetiva ocorrência de resultados danos, frequentemente a vítima está disposta a assumir certos riscos. No ambiente virtual, a navegação diligente se insere no âmbito de organização da vítima, de forma que ela assume determinadas responsabilidades inafastáveis, sob pena de se incorrer em indesejado paternalismo penal.

Não há que se falar de instrumentalização indistinta da vítima diante de quaisquer delitos dolosos praticados no ambiente virtual, como fraude eletrônica e invasão de dispositivo informático, o que apenas pode ser aferido no caso concreto e à luz das circunstâncias subjetivas do usuário. Sob a ótica da teoria da imputação à vítima, pode-se dizer que embora haja deveres objetivos que recaiam sobre o âmbito de organização de qualquer usuário, existirá instrumentalização de determinadas vítimas, como as jovens, idosas e ignorantes, posto que o agente explora uma fraqueza intrínseca em seu desfavor.

Logo, a teoria da imputação à vítima também passa a obter guarida perante os delitos informáticos ao receber influxos criminológicos e político-criminais, posto que muitas vezes os usuários de fato estão dispostos a assumir riscos razoáveis no ambiente virtual.

6.3. Vítima e imputação objetiva

A partir da síntese das teorias funcionalistas ora expostas, é notável que o denominador comum, sob a ótica da vítima, se lastreia na concepção de livre desenvolvimento da personalidade, dotado de cariz constitucional nos principais Estados Democráticos de Direito em que vigora o sistema *civil law*. Com efeito, Roxin, Meliá e outros defensores de teorias funcionalistas mais moderadas verificam que o bem jurídico de seu titular não consiste em um fim em si mesmo, mas se dirige a servir a seu titular, posto que dotado de autodeterminação. Inclusive para a teoria sistêmica de Jakobs, não se pode prescindir do livre desenvolvimento individual, ou seja, da responsabilidade de cada qual como ser autônomo, para se reconhecer a delimitação de âmbitos de organização. Neste ponto, portanto, reside forte diálogo entre teorias vitimodogmáticas e defensores da normativização da conduta da vítima na imputação objetiva.

A teoria funcionalista moderada de Roxin inaugura profundos debates acerca da relevância da vítima na configuração do tipo penal. Ao inserir hipóteses de sua exposição a riscos (auto e heterocolocação) em um terceiro momento de análise (alcance do tipo),

pressupõe-se uma decisão livre e consciente no tocante ao risco, referindo-se apenas a bens jurídicos individuais.[522] [523]

Por outro lado, critica-se que as teorias funcionalistas se limitam a grupos de casos específicos, sem efetiva pretensão de generalização devido a uma carência de critérios. Nesse ponto, como visto, Meliá se aprofunda em sua teoria de imputação à vítima. À contrariedade de Roxin, insere-a no âmbito de criação de risco proibido, apesar de compartimentalizada dos demais elementos dessa fase de imputação. Meliá então busca trazer critérios mais claros acerca da delimitação do âmbito de organização conjunta do autor e vítima a partir de uma abordagem do princípio da autorresponsabilidade.

Muito embora essa construção original de Meliá apresente aplicação restrita, posto que dirigida a condutas nas quais há uma finalidade comum entre autor e vítima – circunscrita em regra a delitos culposos e, quando muito, marcados por dolo eventual –, a sociedade de risco atual passa a permitir a delimitação do âmbito de organização da vítima também ante delitos dolosos, quando digam respeito a bens jurídicos disponíveis que representam o cerne do exercício de liberdades individuais. Assim, perante a autodeterminação informática e delitos patrimoniais, exsurge uma necessária reflexão sobre o papel assumido pela vítima na prevenção delitiva.

Afastando-se do funcionalismo moderado, Jakobs traz novas contribuições ao papel desempenhado pela vítima. Como aponta Meliá, a teoria funcionalista sistêmica de Jakobs peca por excessivo apego ao "sociologismo", ou seja, servidão à situação existente, de modo que a amplitude do conceito de identidade social poderia justificar tanto estados democráticos como autoritários. Por outro lado, jakobs não abdica do alinhamento do direito penal a uma ordem normativa legítima, o que implica reconhecimento de porosidade do sistema e certa abertura a valores.[524] De qualquer modo, como defendido no Capítulo 2.1., a teoria do bem jurídico como

---

[522] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004, p. 138.

[523] Uma das principais críticas dos finalistas sobre o instituto da autocolocação em risco consiste na possibilidade de implicar exclusão típica no tocante a bens jurídicos indisponíveis, notadamente, a vida.
Ocorre que, ao inserir a autocolocação em risco no bojo da teoria da imputação objetiva, Roxin o torna um conceito normativo. Busca, desse modo, a atipicidade de condutas tipificadas por razões paternalistas, como: "moral, tabu, legislação simbólica, sensibilidade da população, ética, proteção de decisões imaturas ou precipitadas, ansiedade, depressão." Trata-se de reconhecer que esse instituto deflui da autodeterminação individual, que perpassa pela livre tomada de decisões. (FEIJÓO SÁNCHEZ, Bernardo José. Actuación de la víctima e imputación objetiva: comentario a la STS del 17 de septiembre de 1999. *Revista de Derecho Penal y Criminología*, n. 5, **p**p. 265–333, 2000, p. 290).

[524] MELIÁ, Manuel Cancio. O estado actual da política criminal ea ciência do Direito Penal In: CALLEGARI, André Luís et al. *Direito penal e funcionalismo*. Trad. André Luís Callegari. Porto Alegre: Livraria do Advogado, p. 89-115, 2005, p. 112.

forma de livre desenvolvimento do indivíduo é aquela que deve ser adotada em um Estado democrático de Direito, de forma a não se acolher o funcionalismo sistêmico de Jakobs.

Apesar das críticas tecidas a Jakobs, sua teoria de ações a próprio risco, desenvolvida a partir do papel social desempenhado por cada indivíduo, consiste em uma coesa tentativa de normatização do princípio da autorresponsabilidade, notadamente no tocante a crimes dolosos. Como reconhece o autor, o âmbito de organização de cada indivíduo se aplica também face a condutas dolosas, nas quais incumbiria à vítima um atuar mais cuidadoso, à luz das expectativas sociais. Sua teoria carece, contudo, de necessário amparo em critérios político-criminais, correndo o risco de se tornar autorreferencial e tautológico.

Nota-se que os estudos funcionalistas conduzem ao reconhecimento de que não apenas o autor é protagonista da conduta punível, mas que também há outros personagens relevantes, notadamente, a vítima. Nesse contexto, os principais representantes das teorias funcionalistas dirigem esforços para a normatização de seu comportamento.

Segundo Mir Puig, o direito ao livre desenvolvimento da personalidade, de cariz constitucional, implica que o ordenamento penal deve permitir a assunção de riscos, ainda que culminem como lesões sob o aspecto naturalístico. Por conseguinte, "indica-se a imputação preferente de tais lesões sobre a vítima, com a consequente exclusão de sua imputação sobre aqueles que intervêm no risco." O critério relevante, nesse contexto, se torna a disponibilidade do bem tutelado: sobre valores disponíveis o raciocínio pode ser aplicado, enquanto deve ser matizado diante de bens indisponíveis – que denotam valores supraindividuais e de ordem pública.

Destarte, o funcionalismo recorre ao livre desenvolvimento do indivíduo em sua perspectiva ativa, de assunção de riscos, para fundamentar o instituto da autocolocação da vítima em risco. Na seara virtual, do memso modo, o funcionalismo cuida da exposição informativa ativa, do usuário que consciente e voluntariamente se expõe a riscos superiores aos já existentes.

No entendimento de Feijóo Sanchez, esse raciocínio conduz necessariamente ao conceito de autorresponsabilidade, a conferir parâmetros para o comportamento do titular do bem jurídico na delimitação do tipo penal. Contudo, em oposição aos defensores da vitimodogmática, o autor defende que esse princípio necessita de concretude normativa para desempenho de sua adequada função na tipicidade. Enquanto a responsabilidade, na ótica vitimodogmática, tem origem fática, esse princípio deve provir de conceitos normativos para

maior concreção. Para tanto, lastreia-se na autodeterminação humana, a partir de um sistema constitucional de liberdades. [525]

Assim, Feijóo Sanchez considera que o fundamento da tipificação de delitos lesivos de bens jurídicos individuais é a afetação do âmbito de organização alheio, de maneira que apenas haverá violação normativa se a pessoa instrumentalizar outrem,[526] mediante uma "dominação de preferência normativa". Logo, em hipóteses de decisão consciente da vítima, seu comportamento de torna um filtro objetivo da responsabilidade no âmbito do tipo. [527]

Nessa linha convergem os critérios delineados por Meliá, sintetizados como a cirscunscrição ao âmbito de organização conjunta perante vítima não instrumentalizada, inexistindo posição de garante. Trata-se de parâmetros objetivos que estabelecem diretrizes para a análise típica. E o preenchimento desses critérios torna-se profícuo por meio de uma aproximação com a política criminal,[528] viabilizando a inserção de teorias criminológicas e da perspectiva vitimológica.

Nos crimes informáticos, a construção funcionalista do âmbito de organização da vítima perpassa pelo arcabouço das teorias criminológicas que despontam na atualidade, notadamente a general theory of crime, teoria das atividades rotineiras e situational crime prevention. Ainda, o perfil das vítimas de delitos informáticos permite perquirir sobre fatores de instrumentalização por parte do agente. Por essa razão, vê-se que as teorias funcionalistas, ao conferir o devido enfoque à conduta da vítima, vão ao encontro do papel protagonista desempenhado pelo usuário no ambiente informático, donde decorrem diversos influxos relevantes para análise da responsabilidade penal.

6.4. Considerações sobre o funcionalismo penal nos crimes informáticos

Apesar de inexorável a expansão do direito penal na sociedade de risco atual, sua procedência deve ser criteriosa e em observância ao princípio da intervenção mínima, essencial ao Estado Democrático de Direito. Destarte, não é facultado ao legislador impor novos tipos

---

[525] FEIJÓO SÁNCHEZ, Bernardo José. Actuación de la víctima e imputación objetiva: comentario a la STS del 17 de septiembre de 1999. *Revista de Derecho Penal y Criminología*, n. 5, pp. 265–333, 2000, p. 307.

[526] Depende em grande medida dos critérios para qualificar como instrumento ou como responsável a pessoa que se lesiona. Um defeito absoluto de responsabilidade (inimputabilidade, erro invencível, inexigibilidade) causado ou sabido por terceiro é imputável a este. A realização do tipo por meio de um instrumento não depende somente do homem de trás, mas também do instrumento, que pode ser apto a evitar a imputação. (FEIJÓO SÁNCHEZ, Bernardo José. *Op. cit.*, p. 302).

[527] Ibidem, p. 298.

[528] Assim, há compatibilidade com o funcionalismo moderado de Roxin e a própria teoria de imputação à vítima de Meliá.

penais - e aos juristas, aplicá-los – caso haja mecanismos não penais acessíveis e igualmente adequados para a prevenção delitiva. Referido raciocínio se aplica integralmente aos ilícitos informáticos, que não necessariamente serão coibidos pela via penal ou pelo simples incremento de sanções – como amplamente visto no Capítulo 4.2. (Criminologia e crimes informáticos).

Nesse contexto, mostra-se salutar o impulso da teoria da imputação objetiva com vistas a refrear a pulsante incidência penal, extirpando-se o crime desde o nível da tipicidade,[529] ou mesmo viabilizando adequada atribuição de responsabilidade, tendo por base o princípio da culpablidade.

Desse contexto também exsurge a importância da participação da vítima, que se torna responsável pela tutela de seus bens jurídicos, de modo a evitar excessiva culpabilização do autor por condutas assimiladas pelo ordenamento jurídico. Está a se falar de verdadeira consagração de valores constitucionais, reconhecendo-se que o livre desenvolvimento do indivíduo no ambiente informático implica a assunção de riscos. Esses riscos não irão culminar com uma necessária lesão ao bem jurídico – autodeterminação informática ou patrimônio -, mas possivelmente com o seu exercício nos ditames da autorresponsabilidade.

Essa contribuição é de extrema valia por meio do alcance do tipo delineado por Roxin, com os já consagrados conceitos de autocolocação e heterocolocação em risco consentida. Do mesmo modo, Meliá traz aportes de caráter dogmático ao reconhecer a incidência desses institutos já no âmbito de criação de um risco proibido. Sua teoria de imputação à vítima traz um aprimoramento de idéias vitimodogmáticas carentes de estruturação na parte geral, sendo apta a conferir maior rigor científico-metodológico.

Em suma, a teoria da imputação objetiva, sob o viés funcionalista moderado, trouxe aportes fundamentais ao reinserir preceitos político-criminais como fator relevante para a conduta típica, de modo a revigorar os clássicos princípios do direito penal e, concomitantemente, propiciar avanços na normativização para a tutela de novos bens jurídicos à luz de seu titular, corroborando com o postulado constitucional do livre desenvolvimento do indivíduo. Do mesmo modo, não se pode descartar por completo a teoria delineada por Jakobs, que traz profícuos raciocínios acerca dos papéis sociais desempenhados pelos indivíduos em sociedade.

Sua contribuição se expande à medida que afloram novos riscos na sociedade do século XXI. Com a disseminação dos meios virtuais, surge um novo ambiente dotado de uma série de

[529] SOUZA, Luciano Anderson de. Direito Penal. v. 1. São Paulo: Revista dos Tribunais, 2019, p. 258.

riscos, muitos dos quais permitidos por carência de regulamentação – situação paulatinamente revertida no país, com o advento do marco Civil na Internet e LGPD – e outros proibidos – com a tutela penal na seara dos crimes informáticos.

Nesse contexto, o viés funcionalista moderado permite influxos das teorias criminológicas alusivas a crimes informáticos, como forma de moldar soluções penais e extrapenais aptas a promover as finalidades preventivas do Direito Penal e, como decorrência, a tutela dos bens jurídicos.

Sob a ótica extrapenal, a teoria das atividades rotineiras aponta para a importância de se providenciar guardiões capazes,[530] o que necessariamente conduz à responsabilidade de que as empresas fornecedoras de dispositivos informáticos e *hardwares* em geral promovam *antimalwares* e *firewalls* adequados e sua constante atualização, impondo-se um regramento normativo para tanto. Ainda, a *situational crime prevention* assinala uma série de medidas com vistas a reduzir o custo-benefício do crime informático para o autor, por exemplo, aprimorando-se o complicance empresarial e enrijecendo a responsabilidade civil e administrativa de provedores de conexão pelo conteúdo divulgado.

Mas é efetivamente na autocolocação em risco em que os crimes informáticos encontram forte contribuição da teoria funcionalista moderada de Roxin, que se mune dos aportes criminológicos na própria conformação da conduta penalmente típica, bem como nos reflexos sobre a dosimetria da pena.

Em suma, como visto, a teoria das atividades rotineiras aponta maior incidência de crimes informáticos: a) em usuários que não ativam ou não possuem *antimalware*s instalados; b) que praticam condutas online tidas por arriscadas, como displicente acesso e compras em *websites* desconhecidos e interações em sites/aplicativos de relacionamento. Esses resultados também são verificados por meio da *situational crime prevention*. Logo, considerando ser necessário desincentivar referidas práticas para finalidades preventivo-penais, esses fatores devem ser incorporados na análise típica e na pena final a ser aplicada.

Crespo reconhece que o "preço da modernidade e dos avanços tecnológicos" consiste na necessária conscientização dos usuários acerca dos riscos na Internet.[531] Reconhece que, à medida que os usuários amadurecem no ambiente digital, com paulatina inclusão digital, abre-

[530] Vide Capítulo 4.3. (Novas propostas criminológicas aos crimes informáticos).
[531] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 108.

se espaço para exigibilidade de condutas que ensejem risco reduzido e/ou permitido à luz da teoria da imputação objetiva. [532]

Dessa forma, há espaço para incidência da autocolocação em risco, notadamente no que pertine a delitos informáticos próprios e impróprios de cunho patrimonial, como furto qualificado mediante fraude por meio de dispositivo informático, fraude eletrônica e estelionato.

De imediato, com o célere avançar tecnológico, pode-se traçar o perfil do homem médio no ambiente virtual, que apresenta padrões e suscetibilidades emocionais a que todos estão sujeitos, sendo-lhe exigíveis cautelas elementares, à luz de sua autorresponsabilidade informática. A correção de desvios ocorre pela análise de elementos subjetivos do usuário, de modo que sobre as vítimas jovens, idosas e tecnologicamente ignorantes não devem recair as exigências do usuário médio.[533]

À medida que progredirem a educação digital e o acesso a dispositivos informáticos à população, haverá maior tendência à objetivização das cautelas mínimas exigíveis dos usuários, padronizando-se o perfil do homem médio virtual. Ocorrerá, assim, maior empoderamento dos usuários, com uniformização do conhecimento informático. Sob a perspectiva preventiva, haverá notáveis benefícios da educação digital, com menor exploração das vulnerabilidades. Ainda, pode-se conduzir a uma reformulação – quer alargamento, quer redução – dos perfis de vítimas solitárias, descuidadas e gananciosas conforme novas medidas preventivas são incorporadas ao arcabouço do usuário.

Em razão da compatibilidade dos postulados político-criminais com a teoria da imputação à vítima de Cancio Meliá também pode ser considerada na seara dos crimes informáticos, permitindo-se delinear o âmbito conjunto de organização da vítima e hipóteses de inexistência de instrumentalização da vítima.

Por fim, a proposta de consolidação do homem médio informático mostra-se profícua para a teoria sistêmica de Jakobs, o que permitirá delinear quais papéis sociais são esperados dos usuários, verificando-se as ações a próprio risco. Assim, muito embora a teoria de Jakobs

---

[532] Se por um lado a autonomia com que cada usuário conduz sua navegação lhe outorga amplo grau de liberdade, por outro, surgem as responsabilidades a ela atreladas nesse ambiente de riscos. Por essa razão, não mais soa utópico falar-se de uma licença internacional para manejo de computador, considerando-se os riscos a que os usuários expõem a si mesmos e a seus pares. (CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 107).

[533] No tocante à vitimização, a *general theory of crime* aponta que pessoas com menor grau de autocontrole se tornam mais suscetíveis a delitos informáticos, enquanto a teoria das atividades rotineiras sinaliza para maior incidência em jovens e pessoas com pouco conhecimento informático. Desse contexto criminológico extrai-se a importância da educação digital para que os usuários abstraiam fatores emocionais do ambiente digital – como a desinibição, excessiva confiança em si e em terceiros –, o que deve se iniciar desde tenra idade.

possa se abstrair de critérios político-criminais, nada obsta que deles se utilize, desvelando certa abertura sistêmica necessária.

A viabilidade de aplicação da teoria funcionalista sobre os crimes informáticos é uma realidade. Contudo, por se tratar se tema pouco desenvolvido, restam muitos desafios para uma adequada estruturação de suas bases. São também necessários mais estudos criminológicos no Brasil, posto que os estudos acerca de delitos informáticos ainda se limitam aos Estados Unidos e à Europa. Com a pulverização de crimes informáticos durante a pandemia de COVID-19, com mais razão tornam-se necessários estudos pátrios, o que de modo algum prejudica as conclusões estrangeiras vislumbradas até o momento.

No Capítulo seguinte, busca-se traçar possíveis caminhos para a solução adequada dos casos concretos sob a ótica da teoria da imputação objetiva moderada de Roxin, tendo por diretriz o delineamento do deilto de estelionato, de modo que a autodeterminação informática e demais bens jurídicos nos crimes informáticos impróprios (notadamente, o patrimônio) se tornam um vetor interpretativo essencial.

6.5. Propostas para a autocolocação em risco nos crimes informáticos

Para fins de compreensão da autocolocação em risco nos crimes informáticos, propõem-se diretrizes para dois bens jurídicos cujo recorte foi determinado nesta pesquisa: a autodeterminação informática e o patrimônio. Em razão de seu caráter individual e disponível, consistem no cerne da manifestação do livre desenvolvimento da personalidade no ambiente virtual. Refletem, com isso, a cristalização da assunção de riscos informáticos como critério apto a gerar repercussões penalmente relevantes.

O patrimônio, compreendido como bem jurídico disponível por excelência no ordenamento constitucional, adquire especial relevância quando da aplicação da teoria da imputação objetiva. Afinal, para além de crimes contra a vida e integridade física, ou mesmo, delitos de imprudência, faz-se mister a hermenêutica daquela teoria com vistas a se delimitarem as condutas penalmente relevantes ao Direito Penal. O papel da vítima ganha especial destaque nos crimes patrimoniais, em que a proteção conferida pela lei penal não deve ser tão abrangente como em delitos contra a vida, à luz da fragmentariedade e subsiariedade penal. Sendo assim, a princípio, a vítima é responsável pelos atos de disposição patrimonial que efetua (princípio da autorresponsabilidade).

No tocante aos crimes informáticos impróprios (mistos, mediatos ou impróprios *stricto sensu*) que atinjam o patrimônio, é viável a integral transposição desse raciocínio,

considerando-se que o emprego do ambiente virtual é apenas um instrumento para o locupletamento ilícito do agente.

Do mesmo modo, no tocante aos crimes informáticos próprios, o bem jurídico autodeterminação informática é disponível por excelência. Tutela, como visto, a autonomia de seu titular ao lidar com seus dados, sendo, por isso plenamente aplicáveis a autoproteção e autorresponsabilidade, como visto no Capítulo 2.3. ((In)Disponibilidade do bem jurídico tutelado).

Na seara pátria, Jesus e Milagre já aventaram a possibilidade de incidência da autocolocação em risco em delitos informáticos, como hipóteses de uso de *hotspot* público sem proteção, uso de senhas fracas, acesso a sites suspeitos e não adoção de *firewall* ou mecanismos de segurança. [534]

Nesse contexto, propõe-se o emprego do referencial paradigmático do delito de estelionato, delito de intervenção por excelência, sob a ótica da imputação objetiva a fim de expandi-lo aos demais crimes informáticos ligados a bens jurídicos disponíveis. Há profícua doutrina sobre o tema, com base na compreensão do engano e fraude que, como visto, permeiam os principais delitos informáticos objeto de estudo.

Aliás, como visto, o elo mais frágil na seara informática é o usuário, que se encontra sujeito a ardis e fraudes. Isso porque a imensa maioria dos delitos de invasão de dispositivo informático, furto qualificado mediante fraude por meio informático, fraude eletrônica e estelionato pode ser evitada por meio de condutas diligentes do usuário do dispositivo. Nesse contexto, em vez de incremento penal e expansão desenfreada de novos tipos penais, é preferível a prevenção delitiva como estretégia de política criminal, o que necessariamente perpassa pela educação digital dos usuários.[535] *Destarte, à luz da teoria da imputação objetiva, guiada pelo viés político-criminal, visa-se a fomentar práticas preventivas dos usuários em detrimento de integral e severa responsabilização penal dos agentes.*

De início, esclarece Sarrabayrouse que os indivíduos são responsáveis por seus atos de disposição sempre e na medida em que essa disposição não seja proveniente de uma conduta enganadora que gera riscos não permitidos pela norma penal.[536] Consequentemente, na hipótese

---

[534] JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016, p. 160.

[535] LEONHARDT, Daniel. Impacto das novas tecnologias sobre a percepção axiológica do Direito penal. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em: https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos. Acesso em: 16 ago. 2021.

[536] Imputación objetiva, fraude inmobiliario y delito de estelionato. In: YACOBUCCI, Guillermo Jorge. *Derecho penal empresario*. Coordenação de Mario H. LAPORTA, Nicolás D. RAMÍREZ. Montevidéu: B. de F., 2010, p. 340. Disponível em: http://201.23.85.222/biblioteca/index.asp?codigo_sophia=78454. Acesso em: 20 mai. 2018.

do delito de estelionato, a transferência da responsabilidade do ato de disposição ao autor apenas pode ocorrer mediante a violação de deveres de veracidade.[537] Desse modo, em razão de sua configuração típica – a qual pressupõe uma conduta do sujeito passivo –, o estelionato se mostra paradigmático na delimitação do comportamento do autor que constituirá uma agressão típica ao patrimônio da vítima, o que levará a implicações em todos os delitos contra o patrimônio.[538]

Conforme preleciona Pastor Muñoz, o tipo penal referente ao estelionato se volta a garantir ao titular do patrimônio certo grau de informação verídica para que seu ato de disposição seja um processo livre de vícios.[539] Portanto, esse tipo penal tem a função de garantir certo grau de orientação ao indivíduo que realizará um ato de disposição patrimonial.

Referido raciocínio pode ser transposto ao delito de fraude eletrônica, posto que a transferência de dados deve ser embasada em um processo livre de seu usuário, o que também se aplica ao delito de furto qualificado mediante fraude por dispositivo informático – de tradicional semelhança com relação ao delito de estelionato.

Do mesmo modo, em crimes informáticos próprios, está a se falar da autodeterminação informática do usuário, ao qual se deve conferir condições adequadas para a tomada autônoma de decisão acerca do tratamento conferido aos dados pessoais.

Há duas elementares fundamentais para a constatação do processo causal do delito de estelionato.[540] Primeiramente, deve existir um erro ou engano causado pelo autor. Em um segundo momento, deve existir um ato de disposição patrimonial pela vítima, o qual implicará

---

[537] Ibidem, pp. 340-341.

[538] Verificam-se duas tendências em busca dessa reposta. Por um lado, nota-se a preponderância da perspectiva do autor, desconsiderando-se a autorresponsabilidade da vítima. Esta torna-se um mero objeto do autor, tratando-se as relações entre os indivíduos como um elemento estático. Por outro lado, há autores que partem da premissa de que a vítima pode ser responsável pelo seu ato de disposição patrimonial, na linha das correntes vitimodogmáticas defendidas por Schünemann e Silva Sánchez. Sob esse prisma, que se entende pelo correto, incumbe identificar o limite de atuação em que a responsabilidade pelo ato de disposição deixa a esfera de responsabilidade da vítima e passa a abrigar aquela do autor. (PASTOR MUÑOZ, Nuria. El redescubrimiento de la responsabilidad de la víctima en la dogmática de la estafa. In: SILVA SÁNCHEZ, Jesús María. *Libertad económica o fraudes punibles: riesgos penalmente relevantes e irrelevantes en la actividad económico-empresarial.* Madrid: Marcial Pons, 2003, pp. 67-68).

[539] PASTOR MUÑOZ, Nuria. *Consideraciones sobre la delimitación del engaño típico en el delito de estafa. Doctrina y jurisprudencia penal, Santiago,* v. 1, n. 1, 2010, p. 46. Disponível em: http://201.23.85.222/biblioteca/index.asp?codigo_sophia=88342. Acesso em: 20 mai. 2018.

[540] A simples afirmação de que o engano no estelionato deve ser a causa - no sentido da teoria da equivalência das condições – para a disposição patrimonial não fornece as soluções adequadas ao plexo de casos. Por isso, "assegurada a relação de causalidade conforme a teoria da equivalência das condições, devem agregar-se critérios corretores de índole normativa que exigem a execução de um perigo por parte do autor e que este não se encontre coberto por um risco permitido dentro do alcance do tipo" (BALMACEDA HOYOS, Gustavo. El delito de estafa: una necesaria normativización de sus elementos típicos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 20, n. 97, pp. 299-364, jul./ago. 2012, p. 320).

causalmente o prejuízo patrimonial.[541] Dessa forma, Pérez Manzano atesta que a criação do risco estará presente nesses dois momentos distintos para se verificar a tipicidade da conduta sob a ótica da teoria da imputação objetiva.[542]

Esse caráter dúplice da tipicidade também é notório nos delitos informáticos ora tratados, em que a vítima é induzida, mediante erro ou engodo, a fornecer dados pessoais (apto a configurar fraude eletrônica), valores (verificando-se o próprio delito de estelionato), ou mesmo a autorizar o acesso a seu dispositivo (incorrendo em furto qualificado mediante fraude ou, caso ausente finalidade patrimonial, eventual invasão de dispositivo informático).

Para a configuração de um risco da conduta típica estelionato, deve-se aferir o engano, compreendido como a falta de verdade no que se diz ou faz. Porém, conforme Donna e Esteban de la Fuente, nem toda mentira proferida pelos agentes consistirá em um engano: cumpre avaliar a idoneidade da fala em efetivamente enganar a vítima.[543] Esses elementos podem ser avaliados, sob a ótica da imputação objetiva, em um juízo de previsibilidade *ex ante*, em que se verifica o risco de a conduta gerar um ato de disposição patrimonial – de dados, ou mesmo de acesso ao dispositivo informático – pela vítima.[544]

Para Nucci, o engano deve ser apto a induzir a erro uma pessoa medianamente cautelosa e prudente, avaliando-se o caso concreto objetivamente. Para tanto, utiliza-se o critério do *homem* médio. Ademais, acrescentam-se as características pessoais da vítima, em uma análise subjetiva da conduta, a fim de se corrigir falhas do critério do homem médio. Em se tratando de pessoa com conhecimentos técnicos específicos sobre determinado assunto, são exigíveis as cautelas que lhe são razoavelmente acessíveis, ainda que superiores àquilo ao alcance do homem médio. Assim, um mero descuido desse sujeito, ainda que dependente de seus conhecimentos específicos, não seria apto a perfazer o tipo penal de estelionato. Do outro lado da moeda, quando se trata de pessoa muito simples ou vulnerável, sem condições de se informar

---

[541] O tipo objetivo de estelionato apresenta três pressupostos: fraude, erro e disposição patrimonial. Esses elementos devem ocorrer nessa ordem, concatenando-se em uma relação de causalidade. Para se evitar uma excessiva amplitude do conceito, esse engano deve limitar-se, por outro lado, à quebra da boa fé no mercado. Considera-se, com isso, o costume social vigente na atividade que se desenvolve. (DONNA, Edgardo Alberto; ESTEBAN DE LA FUENTE, Javier. Algunas reflexiones sobre el concepto de ardid o engaño en la estafa. *Revista de Derecho Penal*, Buenos Aires, n. 1, 2000, p. 483).

[542] PERÉZ MANZANO, Mercedes. Acerca de la imputación obejetiva de la estafa. *Cuadernos de doctrina y jurisprudencia penal*, Buenos Aires, v. 2, 1996, p. 247.

[543]Algunas reflexiones sobre el concepto de ardid o engaño en la estafa, cit., p. 485-486.

[544]PERÉZ MANZANO, Mercedes. *Op. cit.*, p. 250.

de forma adequada, deverá ser reconhecido o estelionato, mesmo diante da abstenção de condutas facilmente acessíveis pelo homem médio.[545]

Sob a ótica da imputação objetiva, nesse sentido convergem os entendimentos de Roxin e Meliá. Jakobs, contudo, entende que deve ser estritamente considerado o papel social desempenhado pelo agente: caso aquele conhecimento específico que possua não esteja integrado ao papel exercido naquele momento, não lhe deve ser exigível o emprego dessa técnica superior. Sua posição, contudo, conduz a injustiças no caso concreto, sendo essencial perquirir-se acerca das características pessoais dos sujeitos envolvidos.

Quanto aos crimes informáticos, o engano do usuário pode estar atrelado ou não a conhecimentos técnicos acerca do ambiente virtual. Em caso afirmativo, deve-se analisar os conhecimentos informáticos do usuário concreto. É notório que no Brasil existem profundas desigualdades sociais que, por sua vez, se refletem no grau de conhecimento sobre a navegação virtual. Contudo, há progressivo aumento de informações sobre a navegação prudente acerca desse ambiente: a) instituições financeiras reiteram que não requerem dados pessoais e senhas por e-mail ou telefonemas; b) emergem orientações pela busca por mecanismos como PagSeguro, assegurando a inviolabilidade dos dados digitados; c) são criadas caixas de *spam*, bem como tachados como suspeitos determinados e-mails recebidos; d) o *firewall* do dispositivo eletrônico acusa arquivos de procedência incerta.

De qualquer modo, tratando-se de vítima ignorante sob a ótica informática, haverá necessariamente sua instrumentalização, de modo que o engano será apto a enganá-la concretamente. Nessa hipótese, convém reiterar a importância da educação digital como fator preventivo extrapenal a ser adotado para se mitigar as causas dos delitos informáticos.

Como visto no Capítulo 4.4. (Proposta de classificação das vítimas informáticas), há também indivíduos particularmente vulneráveis no ambiente informático por suas características pessoais, merecendo destaque os idosos, crianças, adolescentes menores de 14 anos e pessoas com algum grau de deficiência mental.[546] Nessas hipóteses, contudo, deve-se ponderar que nem todos os indivíduos idosos ou jovens padecem de vulnerabilidade virtual. Isso porque é notória a existência de indivíduos jovens extremamente hábeis com dispositivos informáticos, sendo muitos deles *hackers* e *crackers*. Ainda, muitos idosos possuem amplos

[545]Embora o autor não se filie à corrente funcionalista, seus aportes são plenamente aplicáveis, considerando-se, como visto, que o funcionalismo penal não propõe integral superação da teoria finalista. (NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020, p. 494).

[546] Referido raciocínio se mostra compatível com a causa de aumento de pena elencada no artigo 155, §4º-C, inciso II (na hipótese de furto qualificado envolvendo dispositivo informático), que reconhece particular vulnerabilidade a esses grupos.

conhecimentos informáticos e inclusive auxiliaram a desenhar o ambiente virtual tal como é atualmente, de modo que não devem ser abrangidos pela finalidade paternalista indireta da norma penal: afinal, está-se diante de indivíduos dotados de autonomia e capazes de adotar as próprias decisões nesse ambiente. Por conseguinte, é rechaçada uma presunção absoluta de vulnerabilidade (à contrariedade daquela verificada no delito de estupro de vulnerável), para se estabelecer uma presunção relativa, a ser revertida apenas diante da análise do caso concreto – caso se trate, por exemplo, de idoso dotado de conhecimentos informáticos, como Bill Gates.

Por outro lado, é natural que o engano informático explore aspectos psicológicos humanos compartilhados pelo homem médio. Assim, o efeito desinibidor do ambiente informático já deve ser ponderado quando da delimitação do usuário méio digital. Como visto, a *general theory of crime* aponta que menor grau de autocontrole dos usuários conduz a uma maior vitimização. Também há perfis de fraquezas particularmente exploradas, culminando-se com os perfis de vítimas solitárias e gananciosas. Contudo, para fins de aferição de idoneidade do engano, apenas haverá sua incidência se, frente ao homem médio, o usuário apresentar inferior capacidade de autocontrole.

Bitencourt expõe, de modo sintético, as conseqüências decorrentes da i(ni)doneidade do engano, que podem ser aplicadas na teoria funcionalistas:

> É indispensável que o meio fraudulento seja suficientemente idôneo para enganar a vítima, isto é, para induzi-la a erro. A inidoneidade do meio, no entanto, pode ser relativa ou absoluta: sendo relativamente inidôneo o meio fraudulento para enganar a vítima, poderá configurar-se tentativa de estelionato; contudo, se a inidoneidade for absoluta, tratar-se-á de crime impossível, por absoluta ineficácia do meio empregado.[547]

Na seara de delitos informáticos, a idoneidade objetiva de enganar um usuário é extremamente dinâmica, porquanto variável à medida que a sociedade se informatiza. *Websites*, anúncios *e links* falsos, inicialmente aptos a enganar a maioria dos indivíduos, atualmente necessitam de maior sofisticação. Ademais, a narrativa praticada por engenheiros sociais é constantemente atualizada, de modo que se torna paulatinamente obsoleto o golpe do "recebimento de herança" ou do "bilhete premiado". Por esse motivo, é essencial a análise do caso concreto, à luz do usuário objetivamente visado.

Uma vez constatada a idoneidade do engano em induzir o ato de disposição, deve-se excluir os riscos permitidos. Afinal, em muitos setores mercantis é aceitável e recorrente a

[547] BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte especial*. v. 3, 14. ed. São Paulo: Saraiva, 2014, p. 278.

prática de comportamentos inexatos, deformações da verdade, condutas que, em última análise, se enquadram como enganosas. Exageros são marcantes nos mercados e muitas vezes idôneos a levar um indivíduo a um ato de disposição patrimonial. Mantendo-se dentro dos níveis de risco usuais no desenvolvimento da atividade, porém, não há que se falar sequer em estelionato tentado (ou de fraude eletrônica).[548]

Nesse contexto, a edição de parâmetros claros de informação, com base na LGPD, traz diretrizes básicas a serem seguidas quando da obtenção e armazenamento de dados pessoais. A seu turno, não se pode exigir informações profundas e técnicas para além daquelas claramente delineadas nesse diploma normativo.

Ainda, é admissível certa eloquência na venda de produtos no ambiente informático, o que não induz a incidência de estelionato. A título exemplificativo, cite-se o site de vendas *Wish*, em que se vendem produtos aparentemente por preços muito convidativos, porém de dimensões inferiores àquelas esperadas, como cadeiras com 50 cm de altura. Ocorre que basta ler a descrição do produto para aferir suas reais dimensões, o que, contudo, nem sempre está de forma clara e destacada.[549]

Uma vez presente um risco proibido ocasionado pelo engano, a infração do dever de veracidade estabelece uma inversão da ação, em que o agente econômico passa a utilizar o indivíduo como instrumento. Redistribui-se, assim, o risco de erro ou desorientação ao agente econômico.[550]

Ato contínuo, impende verificar se o risco derivado do engano se manifestou efetivamente no ato de disposição da vítima (ou ainda, no fornecimento de seus dados pessoais ou acesso a seu dispositivo informático). O ato de disposição poderá ser distinto ou haver motivos diversos não determinados pelo agente.[551] Convém aferir, nos delitos informáticos

---

[548] Em concreto, é determinante compreender a posição ocupada pelo sujeito no mercado para se aferir o dever de informação. A quantidade de conhecimento que esse sujeito possui é, então, irrelevante. (PASTOR MUÑOZ, Nuria. *Consideraciones sobre la delimitación del engaño típico en el delito de estafa. Doctrina y jurisprudencia penal, Santiago*, v. 1, n. 1, 2010, pp. 49-51). Realmente, em um padrão de mercado atual, marcado pela complexidade e agilidade das relações, mostra-se incabível a exigência de fornecimento de todas as informações ao sujeito passivo, sendo possível apenas exigir um esforço razoável dos agentes econômicos.

[549] Verificada relação de consumo, não haverá qualquer óbice para a reparação civil por meio do Código de Defesa do Consumidor. No entanto, sob a ótica penal, caso não se trate de delito contra as relações de consumo, mas sim de mera índole patrimonial, incidirá a proposta ora apresentada.

[550] PASTOR MUÑOZ, Nuria. *Consideraciones sobre la delimitación del engaño típico en el delito de estafa. Doctrina y jurisprudencia penal, Santiago*, v. 1, n. 1, 2010, p. 50.

[551] Exemplo adaptado de incidência da teoria da imputação objetiva no delito de estelionato. Em troca de e-mails, A induz B a comprar ações X afirmando que sua cotação na bolsa de valores aumentaria. Em verdade, tratava-se de captação de compradores, sendo que a empresa titular das ações irá declarar falência em poucos dias. B solicita ao banco a compra das ações, porém este se equivoca e adquire ações Y, verificando-se acentuada queda destas nos dias subseqüentes. A não deverá responder pelo crime consumado de estelionato. Afinal, o risco criado pelo engano não se manifestou no resultado, tenso sido o ato de disposição e o prejuízo distintos daqueles que o agente visava a obter. (PERÉZ MANZANO, Mercedes. *Op. cit.*, pp. 256-259).

impróprios, se o ato de disposição ocasionado pelo engano efetivamente se manifestou no prejuízo patrimonial. Desse modo, o prejuízo deve ser uma consequência direta daquela disposição do patrimônio. Ora, a vítima pode agir por engano, porém, se sequer houver prejuízo, não há que se falar da consumação do delito.[552] Referido raciocínio se aplica aos crimes informáticos materiais, excepcionando-se os delitos próprios, em que o efetivo prejuízo ou obtenção de vantagem indevida consistem em exaurimento do crime.

Por fim, ressalta-se a importância da atuação da vítima com relação ao alcance do tipo, na visão de Roxin, ou na criação de um risco proibido a partir da conduta da vítima (sob a ótica de funcionalistas como Meliá e Jakobs). Uma vez presente a ciência do sujeito passivo acerca do engano, exclui-se a tipicidade da conduta. Do mesmo modo, em se tratando de vítima gananciosa no ambiente informático, ainda que se trate de engano idôneo, não haverá modalidade consumada do delito caso o usuário busque lucro exacerbado e fácil na aquisição de produtos. Para além dessa hipótese, casos de realização de disposição por pura liberalidade ou negligência grave da vítima não se encontram, igualmente, abarcados pelo fim de proteção da norma.[553]

Por esse motivo, compete ao sujeito passivo informar-se sobre todas as características de funcionamento do mercado de seu interesse, como os preços, existência de outros compradores interessados no produto, entre outros elementos. As características do mercado, é evidente, são essenciais para a delimitação do engano, não sendo assegurada à vítima a proteção diante de sua desinformação por negligência.[554] Trata-se, nessa hipótese, de uma omissão de seu esforço de averiguação, o que implica menores deveres de informação ao agente do mercado.

Ademais, Pastor Muñoz acrescenta que incumbe à vítima averiguar aspectos jurídicos e econômicos da esfera do autor que sejam acessíveis, bem como de seu próprio patrimônio, por se tratar de um esforço razoável e possível para a obtenção de informação.[555] Denomina essa conduta de acessibilidade normativa à informação, em que é possível e esperada ma averiguação prévia pela vítima. Por outro lado, cabe ao próprio agente do mercado informar

---

[552] Ainda no tocante ao exemplo de aquisição de ações, B pode ter adquirido as ações X e estas, ainda assim, aumentarem seu valor. Conforme a concepção pessoal do patrimônio, porém, esse prejuízo não será necessariamente aferível em uma ótica econômica.

[553] Incluem-se aqui negócios de risco calculado ou especulativo, sem comprovar estado patrimonial do solicitante, ou mesmo, relações econômicas entre comerciantes. Visa-se a restringir o alcance do tipo, para não abarcar quaisquer deficiências em cumprimentos contratuais e operações mercantis. (PERÉZ MANZANO, Mercedes. Acerca de la imputación obejetiva de la estafa. *Cuadernos de doctrina y jurisprudencia penal*, Buenos Aires, v. 2, 1996, pp. 259, 263)

[554]PASTOR MUÑOZ, Nuria. *Op. cit.*, p. 56.

[555] Ibidem, p. 55.

dados juridicamente inacessíveis que sejam relevantes para o ato de disposição patrimonial do indivíduo.[556]

A partir das delimitações fincadas pela doutrina com relação à paradigmática hipótese de estelionato, pode-se traçar o alcance do tipo para os delitos informáticos ora tratados. Partindo-se da adoção de critérios político-criminais, impende recorrer às teorias criminológicas propostas na seara virtual (Capítulo 4.3., ao qual se remete o leitor a fim de se evitar repetições desnecessárias), notadamente a teorias das atividades rotineiras e a prevenção situacional do crime, ambas a apontar o papel central do usuário na prevenção de delitos a partir de condutas elementares a seu alcance.

No tocante ao delito de invasão de dispositivo informático, além de furto qualificado mediante fraude por meio de dispositivo informático, são cautelas mínimas aquelas que digam respeito a um esforço razoável a ser exigido do usuário médio. Logo, à exceção de indivíduos particularmente vulneráveis (tanto os presumidamente vulneráveis como, no caso concreto, outros usuários simples e que possuem pouco conhecimento técnico), é necessária a adoção das seguintes condutas, atinentes a uma navegação preventiva: a) atualização constante do sistema operacional do dispositivo; b) instalação, atualização e ativação de *firewall* e *antimalware*s; c) não clicar em links e e-mails sensacionalistas; d) não utilizar dispositivos públicos ou rede pública para acesso a dados sensíveis, como *Internet Banking*;[557] e) manter senhas elaboradas para acesso ao dispositivo e quaisquer logins referentes a dados pessoais; f) verificar a fiabilidade do *website* acessado, ao localizar a presença do elemento HTTPS na URL, bem como a partir de busca simples no "Google" acerca da procedência do site; g) não clicar em links desconhecidos recebidos por e-mail, ou mesmo de teor suspeito, ainda que provenientes de conhecidos.

Quanto aos delitos de fraude eletrônica e estelionato em meio virtual, para além de cautelas mínimas exigíveis do homem médio em seu cotidiano, impõem-se diligências próprias do ambiente informático, notadamente: a) verificar a procedência de *websites* (como sintetizado na alínea "f", acima); b) não adquirir produtos oferecidos por valor muito inferior ao de

[556] Requer-se, ainda, que a vítima aja com diligências mínimas a fim de verificar a veracidade das informações fornecidas pelo agente. Em verdade, em se tratando de imóveis, a vítima tem o dever de consultar pessoalmente o registro da propriedade sempre que, dentro das circunstâncias, haja motivos relevantes para se desconfiar das informações fornecidas pelo vendedor. Ou seja, se houver dúvida razoável quanto à plausibilidade das informações e documentos oferecidos pelo vendedor. Nessas hipóteses, se a vítima opta por não verificar os dados, ela opta por assumir o risco, excluindo-se a incidência do Direito Penal (SARRABAYROUSE, Facundo. Imputación objetiva, fraude inmobiliario y delito de estelionato. In: YACOBUCCI, Guillermo Jorge. *Derecho penal empresario*. Coordenação de Mario H. LAPORTA, Nicolás D. RAMÍREZ. Montevidéu: B. de F., 2010, pp. 345-346).

[557] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 108.

mercado; c) ignorar e excluir e-mails, mensagens e contatos telefônicos provindos de terceiros desconhecidos. Caso aparentem ser verídicos, verificar com redobrada atenção o remetente, sempre se direcionando a sites e contatos oficiais, e não mediante links ou informações fornecidos no bojo da mensagem; d) não fornecer dados e valores a pessoas desconhecidas em sites ou aplicativos de relacionamento.[558]

A aferição da efetiva adoção de diligências mínimas nos crimes informáticos dependerá do caso concreto, considerando-se o grau de sofisticação da fraude e os aspectos particulares do usuário. Caso o usuário médio opte, de forma consciente, por não adotar essas cautelas, poderá ser excluída ou atenuada a imputação ao agente. Se o usuário sequer contempla o risco, caso se trate de conduta relativamente inidônea para enganá-lo (porquanto facilmente perceptível ou evitável, a partir de diligências mínimas, como a instalação de mecanismo de segurança), *o agente responderá apenas pela modalidade tentada, mitigando-se a manifestação do risco proibido no resultado em razão da limitação do alcance do tipo*.

Por outro lado, exclui-se a imputação objetiva, por ausência de incremento de risco, caso se trate de engano grosseiro, evidentemente falso, como aquele que a vítima gananciosa busque explorar. Se o engano for idôneo, porém a fraude for de conhecimento do usuário, haverá exclusão da imputação por não se inserir no alcance do tipo penal. A seu turno, condutas que denotam grau mínimo de negligência ou imprudência podem culminar com singela mitigação das circunstâncias judiciais, à luz do artigo 59, do Código Penal.

Essa gradação dependerá do caso concreto, podendo as diretrizes ser extraídas daquilo já delineado no Capítulo 5.3. (Vitimodogmática e crimes informáticos), evitando-se repetições desnecessárias.[559]

O alcance do tipo das normas ora analisadas é, destarte, a proteção patrimonial e/ou de dados pessoais diante de enganos que levem a atos de disposição de valores ou dados pessoais em dissonância com a autonomia de seu titular.[560]

---

[558] Medidas sintetizadas a partir daquilo exposto no Capítulo 4.3.2., ao qual se remete o leitor.

[559] Desvela-se, neste ponto, certa confluência e semelhança de raciocínio quando comparado com a concepção vitimodogmática. Isso porque, tal como o funcionalismo moderado de Roxin, ao se recorrer a critérios político-criminais, a solução passa a ser orientada a partir das teorias criminológicas vislumbradas, estabelecendo-se matizes da responsabilização penal. A diferença fulcral consiste na proposta de sistematização do funcionalismo, enquanto a vitimodogmática é dotada de maior fluidez. De qualquer modo, a concepção vitimodogmática, por não pressupor necessária ótica funcionalista penal, permitirá a incorporação do raciocínio também por finalistas.

[560] Crespo traz reflexão acerca da distinção entre o consentimento para o resultado lesivo contraposto ao consentimento para o risco, ressaltando que a autocolocação em risco é originalmente voltada a condutas culposas. (CRESPO, Marcelo Xavier de Freitas. *Crimes digitais.* São Paulo: Saraiva, 2011, pp. 107-108). Ocorre que a teoria da imputação objetiva não traz em seu bojo óbices a uma expansão a determinadas condutas dolosas, mormente naquelas em que se pressupõe a atuação da vítima sob engano, como já reconhecido no estelionato.

A normatização almejada pela teoria se opõe a um paternalismo penal, encontrando amparo nos crimes informáticos em razão dos riscos inerentes a esse ambiente e do livre desenvolvimento dos usuários. Simultaneamente, tais medidas adotam um viés preventivo, ao desestimular e desincentivar práticas informáticas fomentadoras de delitos, conforme comprovado por teorias criminológicas.

Logo, quando os usuários se abstêm das cautelas mínimas acima elencadas, dentro da sociedade de risco, não se trata de simples negligência, mas de manifestação de sua indiferença com relação ao resultado danoso, razão pela qual deve ser afastada ou mitigada a imputação ao agente.[561]

A contrario sensu, na esteira daquilo ponderado no Capítulo 5.3, o funcionalismo penal também é apto a ensejar um incremento de pena caso a conduta do agente não só atinja, como também extrapole o alcance do tipo penal acima elencado. Com efeito, caso o usuário adote, além de diligências mínimas, cautelas minuciosas antes da realização do ato de disposição, porém ainda assim seja vítima de um crime informático, deverá incidir maior reprovabilidade sobre o delito praticado em razão de sua maior sofisticação, subvertendo a suposta autonomia do que o usuário supunha possuir em sua decisão. Referido incremento de pena também é criminologicamente aconselhável, posto que se coaduna com a prevenção de delitos informáticos: simultaneamente estimula a adoção de cautelas adicionais pelo usuário e apena com maior rigor o agente que elabora fraudes mais sofisticadas. Esse raciocínio também se expande a delitos informáticos praticados em face de idosos e jovens com idade inferior a 14 anos, alvos em razão de sua presumida vulnerabilidade – dotada de caráter relativo e, como visto, que admite comprovação de conhecimentos técnicos bastantes.

6.5.1. Caso emblemático da torpeza bilateral

Em razão de suas particularidades e ampla incidência no ambiente informático, a compreensão da torpeza bilateral enseja ulteriores explanações. Trata-se de uma expressão mais evidente do exercício ativo do livre desenvolvimento da personalidade dos usuários, demonstrando-se a natureza racional e calculista do ser humano. Com isso, na seara penal, em

[561] É possível estabelecer, destarte, uma analogia com o dolo eventual: a conduta não será meramente culposa, mas dolosa, diante de uma indiferença do agente com relação ao resultado danoso. Uma vez que este raciocínio é aplicado em desfavor do autor, com mais razão deve ser aplicado a seu favor, notadamente porquanto em consonância com o reconhecimento da vítima como ser dotado de autodeterminação, quando oferecidos os elementos adequados para sua atuação.

prol dos princípios da intervenção mínima e culpabilidade haverá impactos mais proeminentes sobre a responsabilidade penal do autor.

No entendimento de Nucci, "cuida-se da situação em que se vislumbra a mesma ânsia de levar indevida vantagem tanto do fornecedor/vendedor quanto do adquirente/comprador."[562]

A posição jurisprudencial e da doutrina pátria dominante aponta para a irrelevância da torpeza bilateral para fins de tipicidade, bastando-se o emprego da fraude e obtenção da vantagem indevida.

Em posição diametralmente oposta, Hungria negava a tutela penal nessas hipóteses, em corrente atualmente endossada por Rogério Greco. Primeiramente, sustentava aquele autor uma compreensão sistemática do ordenamento jurídico, tendo em vista que o próprio Código Civil de 1916 (e, atualmente, o Código Civil de 2002) veda o direito à repetição de valores ou bens ao titular que almejava fim ilício, imoral ou proibido por lei.[563] Ora, se nem sequer o Direito Civil admite indenização diante da torpeza bilateral, com maior razão não deverá interferir o Direito Penal, pautado pelos princípios da fragmentariedade e subsidiariedade.[564]

Ademais, deve-se ponderar que a proteção juridicamente conferida ao patrimônio apenas deve ser direcionada a este enquanto pautado por fins legítimos, sob pena de subversão da própria lógica jurídica de manutenção de expectativas sociais.[565] Por conseguinte, entende-se que, diante da torpeza bilateral, terá predominância a autorresponsabilidade de cada indivíduo, afastando-se a atuação jurídico-penal.

Em uma primeira hipótese, ambos os agentes podem possuir intenção de enganar por meio de alguma fraude. Nucci cita o exemplo de alguém que vende um carro alheio, recebendo o pagamento por meio de cheque furtado. Para além de não se estar diante de prejuízo patrimonial para qualquer dos polos, essa conduta não se amolda ao fim de proteção da norma, posto que a quebra de confiança é fator presente em ambas as partes.[566]

Do mesmo modo, em situações de compactuação de negócio espúrio, imoral e vedado pelo direito, inviável qualquer tutela da norma penal. Carecerá de tutela penal a fraude

---

[562] NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020, p. 495.

[563] Art. 883. do Código Civil: "Não terá direito à repetição aquele que deu alguma coisa para obter fim ilícito, imoral, ou proibido por lei."

[564] HUNGRIA, Nelson.*Comentários ao Código Penal*. Rio de Janeiro: Forense, v. VII, 1955, p. 186. Aproxima-se Hungria, assim, da atual concepção desenvolvida por Zaffaroni no tocante ao conceito de tipicidade conglobante: a análise de uma conduta típica deve transbordar a esfera penal para abarcar todos os ramos do ordenamento jurídico, de maneira que condutas permitidas em outras esferas não poderão ser tidas por ilícitos penais.

[565] Ibidem, p. 187.

[566] NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020, p. 495.

perpetrada em negócios aparentemente legais, porém imorais ou antiéticos. Nesses casos, a vítima, excessivamente gananciosa, busca obter vantagem e lucro fácil em suposta situação de necessidade do agente. Trata-se do famoso golpe do *bilhete premiado*, em que um sujeito se aproxima do ofendido e, após aduzir necessidade ou urgência, propõe a troca do bilhete de lotérica supostamente vencedor por quantia inferior em espécie. A vítima, movida por sua ambição de lucro, opta por obter vantagem sobre o agente, adquirindo o falso bilhete. Nucci também faz menção a estudantes que adquiriram curso junto a suposto estabelecimento de ensino superior em que anunciada a obtenção do diploma universitário no período de uma semana.[567]

Nessas hipóteses, marcadas pelo claro intuito de obtenção de vantagem por meios reprováveis, não há que se falar de incidência do alcance da norma no tocante ao delito de estelionato ou fraude eletrônica.

Há, por fim, hipóteses de elevada especulação que se aproximam da torpeza bilateral, diante de ofertas extremamente vantajosas na aquisição de produtos, normalmente veículos ou eletrônicos. É muito corriqueiro o encontro de anúncios de venda de carros por valor muito inferior ao de mercado.

Como visto, na seara dos delitos informáticos envolvendo patrimônio (notadamente, fraude eletrônica e estelionato), é comum a atuação do usuário movido pela possibilidade de locupletamento rápido, em que figura a vítima gananciosa.[568] Não se pode excluir, a priori, a configuração do delito de estelionato ou fraude eletrônica, sendo necessário analisar as diligências efetuadas pela vítima antes da aquisição e o grau de sofisticação da fraude estruturada pelos agentes (possivelmente muito elaborada, com envolvimento de vários agentes, documentos falsificados, websites). Em uma sociedade liberal e capitalista, não se pode repreender os indivíduos tão somente pelo almejo na obtenção de lucro.

No entanto, do outro lado da moeda, dessa liberdade contratual também deriva o dever de autorresponsabilidade na conclusão dos negócios, a ensejar diligências prudentes do homem

---

[567] NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020, p. 496.

[568] São hipóteses notórias: a) a venda de produtos por preço extremamente baixo, como veículos a 30% do valor de mercado; b) recebimento de herança de um parente desconhecido; c) vencedor de um sorteio do qual sequer participou. Deve-se rechaçar, com isso, o raciocínio de que eventual atipicidade ou mitigação da responsabilidade diante da torpeza bilateral seria contraproducente à já elevada cifra negra que cerca os delitos informáticos. Isso porque, como visto, para fins preventivos mostra-se adequado que os usuários adotem diligências mínimas em suas condutas nesse novo ambiente. Com mais razão, sobre aquele indivíduo que atua com torpeza e contrariamente a propostas preventivas, em pleno exercício de sua autonomia e abstenção de cautelas, não deverá incidir a tutela penal na mesma proporção. Por outro lado, o combate à cifra negra ocorre, em verdade, com o incremento de medidas preventivas, regulação, aparelhamento investigativo e adoção de políticas públicas pelo Estado.

médio. Assim, é possível cogitar-se da inidoneidade do engano, em hipóteses evidentemente fraudulentas levadas a cabo pela vítima gananciosa, bem como da exclusão do alcance do tipo, por autocolocação do usuário em risco. Por fim, é possível reconhecer a imputação, porém com incidência de mera tentativa delitiva, quando a conduta do usuário é permeada por certo grau de negligência, de modo a mitigar a manifestação do risco no resultado em razão da limitação do alcance do tipo, à luz da teoria da imputação objetiva.

CONCLUSÃO

1. A proteção de dados pessoais (informações de caráter personalíssimo que viabilizem a identificação direta ou indireta de seu titular) é construída no ordenamento constitucional como um direito fundamental e da personalidade, sendo decorrente da tutela à honra, intimidade, privacidade e imagem. Sua tutela não se circunscreve ao ambiente virtual, mas nele encontra sua principal manifestação. O reconhecimento explícito desse direito fundamental ocorreu apenas com o advento da Emenda Constitucional n. 115/2022, o que, no entanto, em nada afetou sua consagração prévia de maneira implícita no ordenamento pátrio.

2. A vertente ativa desse direito da personalidade confere enfoque sobre a autonomia do indivíduo, calcada na dignidade da pessoa humana, de modo que a tutela aos dados pessoais no ambiente informático adquire um caráter ativo, tutelando-se sua disponibilidade em prol do livre desenvolvimento do indivíduo. Por essa razão, plasmou-se a "autodeterminação informativa" como regente da LGPD, que passou a ser reconhecida como direito fundamental autônomo pelo Supremo Tribunal Federal em 2020. O indivíduo é, destarte, o centro gravitacional da tutela legislativa na seara informática.

3. Voltando-se à seara penal, impende reconhecer a eclosão de um novo bem jurídico tutelado no ambiente virtual, tripartido nos prismas integridade, confidencialidade e disponibilidade dos dados pessoais, que juntos consubstanciam a autodeterminação informática. Materializa-se com isso o valor constitucional do livre desenvolvimento da personalidade no tocante ao ambiente virtual. Assim, uma exposição informática ativa, com a assunção de riscos informáticos, não implica uma lesão ao bem jurídico ora verificado, mas sim a promoção do desenvolvimento individual à luz da teoria constitucional do bem jurídico.

3.1. Em observância ao princípio da intervenção mínima, a tutela penal a dados pessoais deve se circunscrever ao ambiente informático, dada sua maior essencialidade às atividades dos indivíduos, aliada a seu maior potencial lesivo decorrente de sua instantaneidade e alcance global.

4. Sob a ótica da vítima nos crimes informáticos próprios, verifica-se que a redação atual do artigo 154-A, do Código Penal, conferiu papel protagonista ao titular do bem jurídico tutelado. Embora de modo involuntário – porquanto várias hipóteses de atipicidade derivavam, em verdade, de atecnia e da usual maneira de legislar com base em casos concretos midiatizados –, o legislador atribui à vítima o ônus de se atentar e proteger contra algumas condutas no meio ambiente digital. Em síntese: a) na redação inicial do tipo penal, deveria ser instalado mecanismo de segurança ativado no dispositivo; b) mesmo após a edição da Lei n. 14.155/2021,

a autorização tácita de acesso, inclusive perpetrada mediante artifício, ardil, engodo configura acordo penal e, portanto, conduta atípica; c) a invasão de aplicativos e redes sociais, sem acesso ao dispositivo informático em si, configura conduta atípica.

5. Quanto aos crimes informáticos impróprios patrimoniais, a alteração legislativa promovida pela Lei n. 14.155/2021 foi pontual e marcada por maior rigor nas sanções, sem, contudo, uma preocupação sistemática ou com viés político-criminal. Apesar da nítida violação aos princípios da intervenção mínima e culpabilidade, verifica-se uma preocupação pioneira com a vulnerabilidade das vítimas na seara informática, marcada pelas respectivas causas de aumento previstas no novo delito de furto qualificado, o que apenas inaugura o debate legislativo sobre o tema.

6. No ambiente virtual, a assunção de riscos se torna inevitável, cabendo ao indivíduo a adoção do papel protagonista, quer em razão do caráter intrinsecamente individualista da informática, quer por força do valor constitucional do livre desenvolvimento da personalidade. Esses elementos são particularmente notáveis em se tratando de bens jurídico-penais disponíveis, razão pela qual merecem destaque a autodeterminação informática e o patrimônio.

7. O viés criminológico, particularmente sob a ótica vitimológica, se mostra de premente importância para resgatar o efetivo papel desempenhado pela vítima na gênese delitiva, respeitando-a como ser humano autônomo e dotado de dignidade. Tanto em crimes informáticos próprios como em impróprios, as teorias criminológicas tradicionais não se mostram autossuficientes para uma compreensão global dessa nova modalidade de fenômeno delitivo. Recebem impulso, com isso, propostas direcionadas ao viés virtual.

7.1. A partir da teoria das atividades rotineiras, pode-se extrair fatores aglutinadores de vitimização dos usuários, notadamente: a) pessoas jovens, que adotam condutas virtuais mais arriscadas; b) renda média pessoal superior; c) frequência de navegação em fóruns e redes de relacionamento; d) menor consciência sobre os riscos virtuais; e) maior tempo de conexão do usuário à rede; f) menor uso e atualização de mecanismos de segurança; g) comportamentos virtuais arriscados em geral, como acesso a websites desconhecidos, compras e downloads em páginas inseguras.

7.1.1. Com isso, descartando-se variáveis em que é inviável promover alterações, posto que ligadas a uma exposição informática passiva (como as letras “b” e “e”), há número suficiente de pesquisas embasadas na teoria da atividade rotineira a apontar a importância da adoção de medidas preventivas mínimas pelas vítimas a fim de coibir delitos informáticos.

7.2. Ademais, por meio da teoria da prevenção situacional do crime, extraem-se diversas medidas penais e extrapenais com vistas a uma atuação sistemática na prevenção a crimes informáticos. Dentre as principais propostas, destacam-se a) educação digital da população, com início em fase de escolarização; b) adoção de cautelas mínimas pelos agentes, na linha postulada pela teoria das atividades rotineiras, a fim de se incrementar o esforço percebido pelo agente; c) obrigações legais de aprimoramento de dispositivos informáticos e mecanismos de segurança por parte das plataformas operacionais; d) incremento de atuação de moderadores virtuais de fóruns, bem como da polícia no ambiente virtual para monitoração de atividades ilícitas; e) políticas de compliance efetivo em empresas e no setor público; f) uniformização internacional e cooperação na persecução penal.

7.3. As teorias prevenção situacional do crime e a da atividade rotineira mostram-se profícuas e traçam linhas de estudos criminológicos futuros em razão de sua pretensão de atuação sistemática e global. Seus aspectos são complementares, e várias de suas categorias, intercambiáveis, sendo certo que apontam, dentre seus elementos centrais, para a importância do usuário na prevenção delitiva. Sem sua cooperação, inexistem mecanismos de proteção fática ou jurídica. Isso porque a via alternativa consiste em um incremento de vigilância e redução das liberdades em rede, preço que a sociedade não pode estar disposta a pagar, sob pena de desvirtuamento do Estado Democrático de Direito. Isso, contudo, não significa desamparo dos usuários, posto que várias medidas – notadamente emanadas do Estado – são propostas concomitantemente, merecendo destaque a educação digital e o reconhecimento do acesso à Internet como direito fundamental. Plasma-se, com isso, uma articulação entre o Estado Liberal (em reforço à autonomia individual) e o Estado Social (que fomenta a proteção dos usuários por meio de regulação do ambiente virtual e da educação digital), o que conflui para a atual conformação do Estado Democrático de Direito

8. A indissociabilidade da conduta da vítima na conformação crimes informáticos, conforme relevada pela Criminologia, torna essencial a adoção do viés vitimológico na dogmática penal para a adequada prevenção delitiva. Não se trata de culpabilização da vítima, mas de efetiva observância ao princípio da culpabilidade: o autor apenas deverá responder por aquilo que é obra sua. Do outro lado da moeda, reconhece-se o usuário informático como ser dotado de autonomia, que assume riscos em prol do valor constitucional do livre desenvolvimento de sua personalidade. Nesse contexto, a criminologia traz os necessários embasamentos empíricos norteadores da dogmática penal.

8.1. O devido exercício da autonomia dos usuários perpassa pelo reconhecimento de vulnerabilidades, com destaque para as vítimas ignorantes, jovens e idosas, que devem receber

particular tutela pelo direito penal e extrapenal, com promoção de efetivas políticas públicas de inclusão e educação digital.

9. A vitimodogmática emerge como um dos caminhos possíveis para o reconhecimento do impacto da conduta arriscada do usuário informático sobre a responsabilidade penal do agente. Ao se lastrear no princípio da autorresponsabilidade, fomenta o livre desenvolvimento da personalidade diante dos bens jurídico-penais autodeterminação informática e patrimônio, perquirindo-se por medidas garantistas e que efetivamente fomentem a prevenção penal. Trata-se de uma teoria aplicável por doutrinadores finalistas e funcionalistas, porquanto seu viés fluido e de análise concreta viabiliza amoldá-la a ambas as correntes.

9.1. A corrente majoritária e moderada, ao nosso sentir, peca por excessiva timidez. Em terras pátrias, limita-se a uma dentre as diversas circunstâncias judiciais previstas no artigo 59, do Código Penal, quando da fixação da pena-base. Na seara informática, o papel protagonista dos usuários sob o viés constitucional, reforçado pela perspectiva criminológica, implica conferir maior relevância a suas condutas na seara penal, de maneira que devem ser ponderadas na própria conformação do tipo penal, além de ensejar sopesamento mais relevante quando da dosimetria da pena.

9.2. O raciocínio da corrente minoritária reverbera sobre os delitos informáticos na seguinte medida: usuários que apresentem perfis de vítimas descuidadas, ignorantes ou mesmo solitárias serão desmerecedores de proteção penal diante de prática ou navegação digital negligente ou imprudente. Esse raciocínio, contudo, é demasiado expansivo. Isso porque essa corrente propõe o desmerecimento e a desnecessidade absolutas de tutela caso o titular do bem jurídico (quer se esteja diante da autodeterminação informática, quer do patrimônio) não tenha exercido seus deveres mínimos de cautela no ambiente virtual. Contudo, uma indistinta ausência de responsabilização nessas hipóteses importaria em uma postura informática excessivamente defensiva dos usuários, prejudicial ao exercício e fomento do livre desenvolvimento da personalidade, bem como obstativo de inovações nesse ambiente.

9.3. O caminho mais adequado é a adoção de uma postura vitimodogmática intermediária entre uma recorrente atipicidade e a simples atenuação da pena diante de condutas descuidadas, negligentes ou gananciosas da vítima. Em linhas gerais, essa nova proposta sugere que: a) a ótica vitimodogmática apenas incide em hipóteses nas quais a vítima possui ciência ou estava em condições de saber acerca da existência de um risco concreto ao bem jurídico; b) em qualquer delito permeado por engodo/fraude, se o engano provocado pelo autor não é suficiente a produzir erro sobre a vítima, a conduta será atípica por se tratar de tentativa impossível; c) se o engano for suficiente para provocar o engano, porém a vítima toma ciência

do risco concreto ou estava em condições de sabê-lo, haverá rompimento do nexo de causalidade, respondendo o autor exclusivamente por tentativa, capitulação jurídica em nada maculada por resultado eventual naturalístico danoso.

9.3.1. Amoldando-se esse entendimento aos delitos informáticos, mormente com base na teoria das atividades rotineiras e na prevenção situacional do crime, propõe-se: a) exclusão de tipicidade da conduta, caso o erro ou engano configure crime impossível que a vítima gananciosa leva a cabo em busca de lucro fácil, a partir de condutas elementares legitimamente exigíveis dos usuários; b) responsabilização do autor somente por tentativa caso o usuário possua ciência do risco concreto de sua conduta de navegação na *web* ou fornecimento de dados e valores, como na hipótese de vítimas curiosas e descuidadas; c) atenuação da pena do autor, diante de conduta negligente da vítima, nos termos do artigo 59, do Código Penal, como na exploração de vítimas solitárias em sites de relacionamento. Delineia-se, nesse esteio, uma gradação entre diligências: a) essenciais; b) razoavelmente exigíveis das quais o usuário possui ciência; c) esperadas do usuário médio.

9.3.2. Por outro lado, a tutela penal proposta adota viés mais protetivo às vítimas idosas, jovens e ignorantes, sobre as quais a autorresponsabilidade vitimodogmática recai de forma matizada, com vistas a evitar a culpabilização de usuário que não possui conhecimentos técnicos bastantes para a prevenção delitiva (vítima ignorante) ou que recebe particular tutela pelo ordenamento jurídico em razão de sua vulnerabilidade (vítima idosa e jovem). Quanto a idosos e jovens com idade inferior a 14 anos, fixa-se presunção relativa de matização de sua autorresponsabilidade, que pode ser afastada em se constatando conhecimentos informáticos adequados.

9.3.3. Apesar de ser historicamente voltada a uma mitigação da responsabilidade penal do autor, a vitimodogmática também abre espaço para um incremento de penas a depender da conduta da vítima. Na seara dos crimes informáticos, torna-se criminologicamente aconselhável um incremento da repressão penal (quer via causa de aumento, quer por meio de agravantes) quando se está diante de vítimas extremamente diligentes, bem como idosos e jovens com idade inferior a 14 anos. Nestes últimos, eventuais conhecimentos informáticos da vítima afastam a presunção relativa de vulnerabilidade que deve cercar o acréscimo da pena.

10. Paralelamente à vitimodogmática, no contexto da sociedade de risco e em rede, o funcionalismo penal fornece ferramentas necessárias para a tutela penal de bens individuais e, ainda, traz novos mecanismos aptos à proteção de bens supraindividuais, coletivos ou difusos. Sob a ótica dos delitos informáticos, uma teoria baseada em aspectos puramente ontológicos

não se mostra apta a lidar com aspectos virtuais, que frequentemente não dizem respeito à própria natureza do "ser", mas apenas recebem uma imputação pela via normativa.

10.1. O funcionalismo moderado desponta ao propor uma vinculação entre as decisões político-criminais e a fundamentação do sistema penal, o que propicia uma unidade sistemática e uma atuação prática das ciências criminais, que se voltam tanto à prevenção e redução das causas da criminalidade, como também à mitigação de suas consequências.

10.2. Na seara informática, os estudos criminológicos emergentes conferem embasamentos empíricos concretos para a adoção de um Direito Penal funcionalista genuinamente calcado na realidade. Se, por um lado, se torna criminologicamente desaconselhável um total desamparo penal do usuário, por outro, não se pode incentivar condutas negligentes e displicentes no ambiente informático, o que seria contraproducente sob a ótica criminológica. Como os riscos virtuais emanam do simples fato de se conectar a uma rede, cabe a cada qual a assunção de responsabilidades como forme de livre desenvolvimento de sua personalidade e, apenas assim, será viável a plena promoção dos bens jurídicos autodeterminação informática e do patrimônio.

11. Embora o funcionalismo moderado tenha recebido maior adesão doutrinária, outras teorias funcionalistas trazem aportes relevantes e aptos a influir na teoria do delito, notadamente ao se ponderar que a teoria da imputação objetiva se encontra em constante atualização.

11.1. De particular relevância no funcionalismo sistêmico são as ações a próprio risco: uma ação de forma consciente ou inconscientemente descuidada com os próprios bens pode culminar com uma ação a próprio risco, eximindo de responsabilidade o causador da lesão. De se notar que essa teoria é aplicável tanto a delitos culposos como dolosos, o que amplia seu espectro de incidência. Como critérios, são apontados: a) atividade permanece no âmbito de organização conjunta do autor e da vítima, ou seja, o agente não retira da vítima a autonomia da decisão; b) cognoscibilidade do risco; c) ausência de posição de garante.

11.1.1. A teoria dos papéis sociais do funcionalismo sistêmico permite traçar as responsabilidades incumbentes a cada usuário no ambiente virtual: quais comportamentos são socialmente esperados e quais informações devem ser fornecidas. Apesar de não postular um lastro necessário em critérios político-criminais, a teoria de ações a próprio risco possui âmbito de estudo profícuo em sede de delitos informáticos, delimitando-se o âmbito de organização pertencente a cada usuário do ambiente virtual, o que repercutiria em deveres de diligência por cada qual durante a navegação.

11.2. A teoria de imputação à vítima estabelece três pressupostos essenciais e concomitantes: a) permanência da atividade no âmbito de organização conjunta; b) conduta

autônoma da vítima, sem instrumentalização pelo autor; c) carência de dever de proteção específico do autor frente à vítima (posição de garante). Essa teoria revela-se contida, visto que não delineada para delitos dolosos, apesar de sua idoneidade para explicá-los. Afinal, trata-se de *apurar em que medida a vítima está disposta a assumir riscos de forma razoável*, independentemente do aspecto subjetivo do agente, o que se torna critério relevante para a delimitação do risco permitido na teoria da imputação objetiva. Não há que se falar de instrumentalização indistinta da vítima diante de quaisquer delitos dolosos praticados no ambiente virtual, como fraude eletrônica e invasão de dispositivo informático, o que apenas pode ser aferido no caso concreto e à luz das circunstâncias subjetivas do usuário. Sob a ótica da teoria da imputação à vítima, pode-se dizer que embora haja deveres objetivos que recaiam sobre o âmbito de organização de qualquer usuário, em regra existirá instrumentalização de determinadas vítimas, como as jovens, idosas e ignorantes, posto que o agente explora uma fraqueza intrínseca em seu desfavor.

12. Nota-se que os estudos funcionalistas conduzem ao reconhecimento de que não apenas o autor é protagonista da conduta punível, mas também a vítima. Nesse contexto, o funcionalismo dirige esforços para a normatização de seu comportamento, o que perpassa pela noção de autorresponsabilidade como fator para a promoção do valor constitucional do livre desenvolvimento do indivíduo, notadamente diante de bens jurídicos disponíveis.

13. A construção funcionalista do âmbito de organização da vítima autorresponsável perpassa pelo arcabouço das teorias criminológicas informáticas que despontam na atualidade, notadamente a teoria das atividades rotineiras e *situational crime prevention*. A partir desse aporte político-criminal, a teoria da imputação objetiva permite quais condutas no transpassam a produção de riscos permitidos ou penalmente tolerados normativamente entre os usuários, bem como verificar sua efetiva manifestação no resultado. Nesse estudo, o alcance do tipo merece especial atenção em razão da relevância da navegação diligente dos usuários como modo de prevenção delitiva, sendo apto a se afastar ou mitigar o nexo normativo de imputação em determinadas hipóteses.

14. Para os delitos informáticos alusivos aos bens jurídicos autodeterminação informática e patrimônio, marcados pelo engodo ou fraude perante os usuários, deve-se apurar a idoneidade do artifício empregado para efetivamente enganar a vítima. Se o engano for idôneo, porém a fraude for de conhecimento do usuário, haverá exclusão da imputação por não se inserir no alcance do tipo penal. Caso inidôneo, exclui-se a imputação por ausência de criação ou incremento de risco juridicamente proibido, a título exemplificativo, diante de engano grosseiro, evidentemente falso que a vítima gananciosa busque explorar, como na atuação do

usuário movido pela possibilidade de locupletamento rápido. São hipóteses notórias, que passam a ser praticadas no ambiente virtual: a) a venda de produtos por preço extremamente baixo; b) recebimento de herança de um parente desconhecido; c) vencedor de um sorteio do qual sequer participou. Isso porque, na esteira daquilo apregoado nas ações a próprio risco, bem como na teoria de imputação à vítima, se estará diante do âmbito de organização do próprio usuário, caso ausente posição de garante do agente do qual emanou a fraude.

14.1. Em se tratando de vítimas particularmente vulneráveis sob a ótica informática, notadamente a ignorante, idosa e jovem, haverá em regra sua instrumentalização, de modo que a fraude será apta a enganá-la concretamente. Propõe-se uma presunção relativa de vulnerabilidade diante de idosos e jovens com idade inferior a 14 anos, de modo que uma análise casuística será apta a demonstrar eventuais conhecimentos informáticos equivalentes ou superiores ao do homem médio.

14.2. Caso se trate de conduta relativamente inidônea para enganar o usuário médio (porquanto facilmente perceptível ou evitável a partir de diligências mínimas, como a instalação de mecanismo de segurança), o agente responderá apenas pela modalidade tentada, mitigando-se a manifestação do risco proibido no resultado em razão da limitação do alcance do tipo. A seu turno, condutas que denotam grau mínimo de negligência ou imprudência podem culminar com singela mitigação das circunstâncias judiciais, à luz do artigo 59, do Código Penal. Essa distinção dependerá do caso concreto, podendo as diretrizes ser extraídas daquilo delineado no Capítulo 5.3. (Vitimodogmática e crimes informáticos).

14.3. O alcance do tipo das normas ora analisadas é, destarte, a proteção patrimonial e/ou de dados pessoais diante de enganos que levem a atos de disposição de valores ou dados pessoais em dissonância com a autonomia de seu titular. Deve-se ponderar que a aferição da efetiva adoção de diligências mínimas nos crimes informáticos dependerá do caso concreto, considerando-se o grau de sofisticação da fraude e os aspectos particulares do usuário.

14.4 O funcionalismo penal viabiliza uma compreensão holística da vítima, de modo que enseja um incremento de penas caso a vítima adote diligências acima daquelas usualmente esperadas do usuário médio: sob a ótica político-criminal, incentiva a diligência dos usuários ao passo que desestimula maior grau de sofisticação de fraudes. Referido raciocínio também se estende a vítimas idosas e jovens com idade inferior a 14 anos, que se tornam alvos de crimes informáticos em razão de sua vulnerabilidade, dotada de presunção relativa.

15. Independentemente do caminho adotado, vitimodogmático ou funcionalista, o grau de relevância do usuário no ambiente informático conduz ao seu maior protagonismo na

conformação da conduta penalmente típica, como forma de observância ao preceito constitucional do livre desenvolvimento da personalidade na sociedade informática de risco.

As soluções apontadas, a seus turnos, não possuem pretensão de esgotar a temática, recentemente inaugurada. O caminho na seara informática é pavimentado a partir de perspectivas gerais, porém trilhado à luz do usuário concreto, aporte essencial, aliás, sedimentado por meio da vitimologia e de critérios político-criminais.

A partir de novos estudos criminológicos, será relevante uma constante análise das nuances de cada delito: para delitos informáticos impróprios, os caminhos são bem próximos ao tradicionalmente delineado pelo estelionato. Para delitos próprios, algumas diretrizes básicas são traçadas a partir de suas semelhanças com delitos tradicionais, porém outras poderão ser adotadas à medida que haja melhor regulamentação e inclusão digital dos usuários.

REFERÊNCIAS

Obras

AGUSTINA, Jose R. Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, v. 9, n. 1, 2015.

ALEGRÍA, Gíner et al. Aproximación psicológica de la victimología. *Revista derecho y criminología*, n. 1, 2011.

ALSHALAN, A. *Cybercrime fear and victimization: An Analysis of a National Survey*. Mississipi : Mississipi State University, 2006.

AROCENA, Gustavo Alberto. Acerca del principio de legalidad penal y de hackers, crackers, defraudadores informáticos y otras rarezas. *Ley, Razón y Justicia*, v.4, n. 6, 2002.

ASSARUT, Nuttapol *et al.* Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. *International Journal of Cybercriminology*, v. 13, n. 1, p. 84-100, 2019.

AZIZ, Ashar. *System and method of containing computer worms*. U.S. Patent n. 8,549,638, 1 out. 2013.

BALMACEDA HOYOS, Gustavo. El delito de estafa: una necesaria normativización de sus elementos típicos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 20, n. 97, p. 299-364, jul./ago. 2012.

BECCARIA, Cesare. *Dos delitos e das penas*. Trad. Luciana Guidicini e Alessandro Contessa. São Paulo: Martins Fontes, 2005.

BECHARA, Ana Elisa Liberatore Silva. O rendimento da teoria do bem jurídico no direito penal atual. *Revista Liberdades*, v. 1, n.1, pp. 16-29, 2009.

BECHARA, Ana Elisa Liberatore Silva. *Bem jurídico-penal*. São Paulo: Quartier Latin, 2014.

BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. Tradução: Sebastião Nascimento. São Paulo: Editora 34, 2011.

BEEBE, Nicole Lang; RAO, V. Srinivasan. Using situational crime prevention theory to explain the effectiveness of information systems security. In: *Proceedings of the 2005 SoftWars Conference*, Las Vegas, NV, pp. 1-18, 2005.

BERISTAIN, Antonio. *Nova criminologia à luz do direito penal e da vitimologia*. Brasília: Editora Universidade de Brasília, 2000.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte Geral.* 19. ed. São Paulo: Saraiva, 2012.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte especial*. v. 2, 14. ed. São Paulo: Saraiva, 2014.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal: Parte especial*. v. 3, 14. ed. São Paulo: Saraiva, 2014.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. São Paulo: Saraiva Educação, 2015.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 12, n. 47, p. 146-187, mar./abr. 2004. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=47428. Acesso em: 13 set. 2020.

BOSSLER, Adam. Contributions of criminological theory to the understanding of cybercrime offending and victimization. In: LEUKFELDT, Rutger; HOLT, Thomas J. *The Human Factor of Cybercrime.* New York: Routledge, 2019.

BOSSLER, A. M.; HOLT, T. J. The Effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, v. 38, pp. 227-236, 2010.

BRASIL. Constituição da República Federativa do Brasil de 1988. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 dez. 2019.

BRASIL. Decreto n. 592, de 06 de julho de 1992. Pacto Internacional sobre Direitos Civis e Políticos. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 07 de julho de 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 19 dez. 2019.

BRASIL. Decreto-Lei n. 2.848, de 07 de dezembro de 1940. Código Penal. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 31 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 19 dez. 2019.

BRASIL. Decreto-Lei n. 3.689, de 03 de outubro de 1941. Código de Processo Penal. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 13 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 19 dez. 2019.

BRASIL. Emenda Constitucional n. 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF, 11 de fevereiro de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 10 mar. 2022.

BRASIL. Lei n. 4.737, de 15 de julho de 1965. Código Eleitoral. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 19 de julho de 1965. Disponível em:

https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965. Acesso em: 19 dez. 2019.

BRASIL. Lei n. 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 16 de julho de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 19 dez. 2019.

BRASIL. Lei n. 9.100, de 29 de setembro de 1995. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 02 de outubro de 1995. Disponível em: https://presrepublica.jusbrasil.com.br/legislacao/111051/lei-9100-95. Acesso em: 19 dez. 2019.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 25 de julho de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 19 dez. 2019.

BRASIL. Lei n. 9.504, de 30 de setembro de 1997. Código Eleitoral. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 1º de outubro de 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 19 dez. 2019.

BRASIL. Lei n. 10.741, de 1º de outubro de 2003. Estatuto do Idoso. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 03 de outubro de 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em: 19 dez. 2019.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Lei Carolina Dieckmann. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 03 de dezembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 dez. 2019.

BRASIL. Marco Civil da Internet. Lei n. 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 set. 2021.

BRASIL. Lei Geral de Proteção de Dados (LGPD). Lei n. 13.709, de 14 de agosto de 2018. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 set. 2021.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 28 de maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 19 dez. 2019.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6387, Plenário, relatora Ministra Rosa Weber. Brasília, DF. *DJe de 12 de novembro de 2020*. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 28 dez. 2021.

BREWER, Russell et al. *Cybercrime prevention: Theory and applications*. Springer Nature, 2019.

BRIAT, Martine. La fraude informatique: une approche de droit compare. *Révue de Droit Pénal et Criminologia*, Bruxelles, n. 4, 1985.

BRITO, Auriney. *Direito Penal Informático.* São Paulo: Saraiva, 2013.

BRITO, Auriney Uchôa de. O bem jurídico-penal dos delitos informáticos. *Boletim IBCCRIM*, São Paulo, v. 17, n. 199, pp. 14-15, jun. 2009. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=71060. Acesso em: 15 ago. 2020.

BUSTOS RAMIREZ, Juan. *Introducción al Derecho Penal***.** Bogotá: Editorial Temis. 2. ed, 1994.

CABETTE, Eduardo Luiz Santos. Torpeza ou fraude bilateral no estelionato sob a ótica da vitimodogmática e da autoproteção. *Revista Síntese de direito penal e processual penal*, Porto Alegre, v. 19, n. 115, pp. 59-63, abr./mai. 2019. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigosophia=150328. Acesso em: 6 jan. 2021.

CAMARGO, Antonio Luís Chaves. *Imputação objetiva e Direito Penal*. São Paulo: Cultural Paulista, 2002.

CÁRDENAS, Alvaro E. Márquez. La victimologia como estudio: redescubrimiento de la víctima para el proceso penal. *Revista Prolegómenos. Derechos y Valores De La Facultad De Derecho*, v. 14, n. 27, pp. 27-42, 2011.

CASSANTI, Moisés de Oliveira. *Crimes virtuais, vítimas reais.* Rio de Janeiro: Brasport, 2014.

CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura. São Paulo: Paz e Terra, v. 3, 1999.

CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roneide Venancio Majer. V.1. 6. ed. São Paulo: Paz e Terra, 2011.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: Castells, Manuel; Cardoso, Gustavo (orgs). *A sociedade em rede: do conhecimento à acção política*. Lisboa: INCM, 2006.

CASTELLS, Manuel. *The Internet Galaxy: reflections on the lnternet, business and society*. New York: Oxford University Press, 2001.

CAVALCANTE, Márcio André Lopes. Comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático. 2012. Disponível em: https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html. Acesso em: 07 out. 2021.

CHOI, Kyung-shick. Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, v. 2, n. 1, 2008.

COHEN, Lawrence E.; FELSON, Marcus. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, pp. 588-608, 1979.

CONSELHO DA EUROPA. *Convenção sobre o Cibercrime*, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 set. 2021.

CORNISH, D.V.; CLARKE, R.V. Oportunities, precipitator and criminal decisions. A reply to Wrtley's citique of situational crime prevention. In : SMITH, M.; CORNISH, D.B. (coords.).*Theory for Practice in Situational Crime Prevention*, v. 16, New York, Monsey: Criminal Justice Press, 2003.

COSTA, Adriano Sousa; FONTES, Eduardo; HOFFMANN, Henrique. Lei 14.155/21 incrementa punição de crimes eletrônicos e informáticos. *Consultor Jurídico*, mai. 2021. Disponível em: https://www.conjur.com.br/2021-mai-28/opiniao-lei-1415521-incrementa-punicao-crimes-eletronicos-informaticos. Acesso em: 30 set. 2021.

COSTA, Helena Regina Lobo da. *Proteção penal ambiental: viabilidade, efetividade, tutela por outros ramos do direito.* São Paulo: Saraiva, 2010.

COSTA ANDRADE, Manuel da. *Consentimento e Acordo em Direito Penal*. Coimbra: Coimbra, 2004.

CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011.

CRESPO, Marcelo Xavier de Freitas. Dos crimes de inserção de dados falsos em sistemas de informação (Art. 313-A, CP) e modificação ou alteração não autorizada de sistema de informação (Art. 313-B, CP). *In:* CRESPO, Marcelo Xavier de Freitas (coord.). *Crimes contra a administração pública: aspectos polêmicos*. São Paulo: Quartier Latin, 2010.

DA PONTE, Antonio Carlos. *Crimes eleitorais*. São Paulo: Saraiva, 2008.

DE LIMA, Cintia Rosa Pereira; RAMIRO, Lívia Froner Moreno. Direitos do Titular dos Dados Pessoais. In: De Lima, Cíntia Rosa Pereira (coord). *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020.

DE TEFFÉ, Chiara Spadaccini; DE MORAES, Maria Celina Bodin. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Pensar-Revista de Ciências Jurídicas*, v. 22, n. 1, pp. 108-146, 2017.

DEUTSCHLAND. Bundesverfassungsgericht. Verfassungsbeschwerde n. 209/83, 484/83, 440/83, 420/83, 362/83, 269/83, 1. Senat, Karlsruhe, 15 dez. 1983. Disponível em: http://www.bverfg.de/e/ rs19831215_1bvr020983.html. Acesso em: 29 set. 2021.

DEUTSCHLAND. Bundesverfassungsgericht. Verfassungsbeschwerde n. 370/07, 1. Senat, Karlsruhe, 27 feb. 2008. Disponível em: http://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em: 29 set. 2021.

D'URSO, Luiz Augusto Filizzola. Crimes praticados pelas redes sociais: Induzimento ao suicídio, à autolesão corporal e os crimes contra a honra. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em:

https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos. Acesso em: 16 ago. 2021.

DONNA, Edgardo Alberto; ESTEBAN DE LA FUENTE, Javier. Algunas reflexiones sobre el concepto de ardid o engaño en la estafa. *Revista de Derecho Penal*, Buenos Aires, n. 1, 2000.

DONINI, Massimo et al. *El derecho penal frente al los desafíos de la modernidad*. Lima: Ara Editores, 2010.

EBERT, Udo. Verbrechensbekämpfung durch Opferbestrafung? *Juristenzeitung*, v. 38, n. 17, pp. 633-643, 1983.

EIFERT, Martin. Informationelle Selbstbestimmung im Internet: Das BVerfG und die Online-Durchsuchungen. *Neue Zeitschrift für Verwaltungsrecht*, v. 521, 2008.

EMBLETON, Shawn; SPARKS, Sherri; ZOU, Cliff C. SMM rootkit: a new breed of OS independent malware. *Security and Communication Networks*, v. 6, n. 12, pp. 1590-1605, 2013.

FEIJÓO SÁNCHEZ, Bernardo José. Actuación de la víctima e imputación objetiva: comentario a la STS del 17 de septiembre de 1999. *Revista de Derecho Penal y Criminología*, n. 5, **p**p. 265–333, 2000.

FEILY, Maryam; SHAHRESTANI, Alireza; RAMADASS, Sureswaran. A survey of botnet and botnet detection. In: *2009 Third International Conference on Emerging Security Information, Systems and Technologies*. IEEE, p. 268-273, 2009. Disponível em: http://www.itk.ilstu.edu/faculty/ytang/botnet/3%202009-A%20Survey%20of%20Botnet%20and%20Botnet%20Detection.pdf. Acesso em: 28 set. 2021.

FRANÇA, Leandro Ayres. Cibercriminologias. In: FRANÇA, Leandro Ayres; CARLEN, Pat (orgs.). *Criminologias alternativas.* Porto Alegre: Canal Ciências Criminais, pp. 221-249, 2017.

FRANÇA, Leandro Ayres. Cibercriminologias. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em: https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos. Acesso em: 07 out. 2021.

FROMMEL, Monika. Opferschutz durch hohe Strafdrohungen: Der vergiftete Apfel vom Baume des Punitivismus. *Monatsschrift für Kriminologie und Strafrechtsreform*, v. 68, pp. 350-359, 1985.

GALÁN MUÑOZ, Alfonso. Mitos y realidades de la delincuencia informática. Un estudio sobre la reforma del Código Penal brasileño en materia de delitos informáticos, a la luz del Derecho penal Internacional. *Revista justiça e sistema criminal*: modernas tendências do sistema criminal, Curitiba, v. 1, n. 1, pp. 57-98, jul./dez. 2009. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=89162. Acesso em: 22 jul. 2021.

GOTTFREDSON, M. R. ; HIRSCHI, T. *A general theory of crime.* Stanford, CA: Stanford University Press, 1990.

GOVERNO FEDERAL. Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à Internet. *Site do Governo Federal***.** 14 de abril de 2021. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=IBGE-,Pesquisa%20mostra%20que%2082%2C7%25%20dos%20domic%C3%ADlios,brasileiros%20t%C3%AAm%20acesso%20%C3%A0%20internet&text=A%20popula%C3%A7%C3%A3o%20brasileira%20est%C3%A1%20cada,Geografia%20e%20Estat%C3%ADstica%20(IBGE). Acesso em: 04 out. 2021.

GRABOVSKY, Peter N, Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, v. 10, n. 2, pp. 243-249, 2001.

GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. *A autocolocação da vítima em risco*. São Paulo: Revista dos Tribunais, 2004.

GRECO, Luís. Comentário ao estudo de Schünemann "o direito penal é a ultima ratio da proteção de bens jurídico: sobre os limites invioláveis do direito penal em um estado de direito liberal". *In:* IBCCRIM. INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS *et al*. *IBCCRIM 25 anos*. Belo Horizonte: D'Plácido, 2017.

GRECO, Luis. Introdução à dogmática funcionalista do delito. Em comemoração aos trinta anos de "Política Criminal e Sistema JurídicoPenal", de Roxin. *Impresso do I Congresso de Direito Penal e Criminologia*. UFBA, painel "Funcionalismo no Direito Penal", 13-15 de abril de 2000.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a Internet. *Boletim IBCCRIM*, São Paulo, edição especial, ano 8, n. 95, 2000.

GUARDIA, Diego L. Los delitos informáticos frente al concepto tradicional de "cosa". *Ciencias Penales Contemporáneas*: Revista de Derecho Penal, Procesal Penal y Criminología, Mendoza, v. 2, n. 4, pp. 145-181, 2002.

HASSEMER, Raimund. *Schutzbedürftigkeit des Opfers und Strafrechtsdogmatik. Zugleich ein Beitrag zur Auslegung des irrtumsmerkmals in § 263 StGB*. Berlin: Duncker & Hublot, 1981.

HASSEMER, Winfried. Consideraciones sobre la víctima del delito. *Anuario de Derecho Penal y Ciencias Penale***s,** Madrid, v. 43, n. 1, pp. 241-259, 1990.

HASSEMER, Winfried; CONDE, Francisco Muñoz. *Introducción a la criminología y al derecho penal*. Valencia: Tirant lo blanch, 1989.

HINDELANG, Michael J.; GOTTFREDSON, Michael R.; GAROFALO, James. *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger, 1978.

HOLT, T. J.; BURRUSS, G. W.; BOSSLER, A. M. Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, v. 62, pp. 1720–1741, 2018.

HOFFMANN-RIEM, Wolfgang. Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzer informationstechnischer Systeme. *Juristenzeitung*, vol. 21, n. 1, p. 1009-1022, 2009.

HUNGRIA, Nelson.*Comentários ao Código Penal.* Rio de Janeiro: Forense, v. VII, 1955.

JAKOBS, Günther. *A imputação penal da ação e da omissão*. Barueri: Editora Manole, 2003.

JAKOBS, Günther; CONTRERAS, Joaquín Cuello. *Derecho penal, parte general: fundamentos y teoría de la imputación*. Madrid: M. Pons, 1997.

JESCHECK, Hans-Heinrich. *Tratado de Derecho Penal: parte general*. Barcelona: Bosch, 1981.

JESCHECK, Hans-Heinrich; WEIGEND, Thomas. *Lehrbuch des Strafrechts.* 4. ed, Berlim: Duncker und Hublot, 1988.

JESCHECK, Hans-Heinrich; WEIGEND, Ewa. *Tratado de derecho penal: parte general.* Granada: Comares, 2003.

JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016.

KIRDA, Engin *et al*. Behavior-based Spyware Detection. In: *Usenix Security Symposium*, pp. 273-288 of the Proceedings, 2006. Disponível em: https://www.usenix.org/legacy/event/sec06/tech/full_papers/kirda/kirda_html/ . Acesso em 28 set. 2021.

KINDHÄUSER, Urs; CARO JOHN, José Antonio; GARCÍA CAVERO, Percy. *Estudios de derecho penal patrimonial.* Lima: Grijley, 2002. Disponível em: http://201.23.85.222/biblioteca/index.asp?codigo_sophia=72303. Acesso em: 20 mai. 2018.

KRANENBARG, Marleen Weulen. Contrasting cyber-dependent and traditional offenders : a comparison on criminological explanation and potential prevention methods. In: LEUKFELDT, Rutger; HOLT, Thomas J. *The Human Factor of Cybercrime*. New York: Routledge, 2019.

LEONHARDT, Daniel. Impacto das novas tecnologias sobre a percepção axiológica do Direito penal. In: *Curso de Direito Digital e Crimes Informáticos*, São Paulo: IBCCRIM, 2020. Disponível em: https://play.ibccrim.org.br/cursos/exibir/21/direito-digital-e-crimes-informaticos . Acesso em: 16 ago. 2021.

LEUKFELDT, Rutger; JANSEN, Jurjen. Financial cybercrimes and situational crime prevention. In: LEUKFELDT, Rutger; HOLT, Thomas J. *The Human Factor of Cybercrime*. New York: Routledge, 2019.

LEUKFELDT, Eric Rutger; YAR, Majid. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, v. 37, n. 3, pp. 263-280, 2016.

LYNETT, Eduardo Montealegre. Introdução à obra de Günther Jakobs. In: CALLEGARI, André Luís et al. *Direito penal e funcionalismo*. Trad. André Luís Callegari. Porto Alegre: Livraria do Advogado, 2005.

LÓPEZ DÍAS, Claudia. Acciones a próprio riesgo. *Revista CENIPEC*, v. 25, n. 1, pp. 115-174, 2006.

LUISI, Luiz. *Os princípios constitucionais penais*. Porto Alegre: Ed. Sérgio Antônio Fabris, 1991.

LUZON PENA, Diego-Manuel. Principio de Alteridad o de Identidad vs. Principio de Autorresponsabilidad. Participacion en Autopuesta en Peligro, Heteropuesta en Peligro Consentida y Equivalencia: El Criteria del Control del Riesgo. *Nuevo Foro Penal*, v. 74, n. 6, pp. 58-80, 2010.

MARCUM, C. D. Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, v. 2, n. 2, pp. 346-367, 2008.

MARTINS, Flavio. *Curso de direito constitucional*. São Paulo: Saraiva Educação, 2021.

MARTINS, Leonardo (org). *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Trad. Beatriz Hennig; Leonardo Martins; Mariana Bigelli de Carvalho; Tereza Maria de Castro e Vivianne Geraldes Ferreira. Montevidéu: Konrad Adenauer, 2005.

MATA y MARTIN, Ricardo M. Criminalidad Informática: uma introducción al cibercrimen. In: RUIZ MIGUEL, Carlos et al. *Temas de Direito da Informática e da Internet*. Coimbra: Coimbra, 2004.

MELIÁ, Manuel Cancio. *Conducta de la víctima e imputación objetiva en Derecho penal.* Tese de Doutorado. Universidad Autónoma de Madrid, 1997.

MELIÁ, Manuel Cancio. O estado actual da política criminal ea ciência do Direito Penal In: CALLEGARI, André Luís et al. *Direito penal e funcionalismo*. Trad. André Luís Callegari. Porto Alegre: Livraria do Advogado, pp. 89-115, 2005.

MENDELSOHN, Benjamín. La victimología y las tendencias de la sociedad contemporánea. *ILANUD al día*, v. 4. n. 10, 1981.

MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira*, v. 5, n. 1, pp. 781-809, 2019.

MERINO HERRERA, Joaquín. *Tendencias de la política criminal contemporânea*. Madrid: Marcial Pons, 2018.

MIR PUIG, Santiago. *Introducción a las bases del derecho penal*. Montevideo: B de f. 2. ed., 2003.

MIR PUIG, Santiago. Límites del normativismo em Derecho Penal. *Revista Electrónica de Ciencia Penal y Criminologia*, v. 7, n. 18, pp. 1-24, 2005.

MIRÓ LLINARES, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012.

MITNICK, Kevin D.; SIMON, William L. *A arte de enganar*. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003.

MOCCIA, Sergio. *El derecho penal entre ser y valor: función de la pena y sistemática teleológica.* Buenos Aires: Julio César Faira, 2003.

MOLINA, Antonio Garcia-Pablos de; GOMES, Luiz Flávio. *Criminologia***.** São Paulo: Revista dos Tribunais, 2002.

MOURA, Grégore Moreira de. *Curso de Direito Penal Informático*. Editora D'Plácido: São Paulo, 2021.

NGO, Fawn T.; PATERNOSTER, Raymond. Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, v. 5, n. 1, 2011.

NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 2, 4. ed. Rio de Janeiro, Forense, 2020.

NUCCI, Guilherme de Souza. *Curso de Direito Penal: Parte Especial*. v. 3, 4. ed. Rio de Janeiro, Forense, 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 29 set. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Resolução n. 40/34, de 29 de novembro de 1985. *Declaração dos Princípios Básicos de Justiça Relativos às Vítimas da Criminalidade e de Abuso de Poder*, 1985. Disponível em: http://www.direitoshumanos.usp.br/index.php/Direitos-Humanos-na-Administra%C3%A7%C3%A3o-da-Justi%C3%A7a.-Prote%C3%A7%C3%A3o-dos-Prisioneiros-e-Detidos.-Prote%C3%A7%C3%A3o-contra-a-Tortura-Maus-tratos-e-Desaparecimento/declaracao-dos-principios-basicos-de-justica-relativos-as-vitimas-da-criminalidade-e-de-abuso-de-poder.html. Acesso em: 29 set. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Resolução A / HRC / C / L.20, de 27 de junho de 2016. *A promoção, proteção e gozo dos direitos humanos na Internet*, 2016. Disponível em: https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20. Acesso em: 28 dez. 2021.

ORWELL, George. *1984*. São Paulo: Companhia das Letras, 2009.

OTTO, Harro. *Grundkurs Strafrecht: Allgemeine Strafrechtslehre*, Berlin: De Gruyter, 2004.

PASTOR MUÑOZ, Nuria. *Consideraciones sobre la delimitación del engaño típico en el delito de estafa. Doctrina y jurisprudencia penal, Santiago*, v. 1, n. 1, 2010.

PASTOR MUÑOZ, Nuria. El redescubrimiento de La responsabilidad de La víctima em La dogmática de La estafa. In: SILVA SÁNCHEZ, Jesús María. *Libertad económica o fraudes punibles: riesgos penalmente relevantes e irrelevantes en la actividad económico-empresarial.* Madrid: Marcial Pons, 2003.

PRADO, Luiz Regis. A imputação objetiva no direito penal brasileiro. **Ciências Penais**: Revista da Associação Brasileira de Professores de Ciências Penais, São Paulo, v. 2, n. 3, pp. 81-110, jul./dez. 2005.

PERÉZ MANZANO, Mercedes. Acerca de la imputación obejetiva de la estafa. Cuadernos de doctrina y jurisprudencia penal, Buenos Aires, v. 2, 1996.

PEREZ MANZANO, Mercedes. Acerca de la Imputación Objetiva de la Estafa. In: AA.VV., Hacia un Derecho Penal Económico Europeo, Madrid: BOE, 1995.

PRATT, T. C. *et al. Self-control and victimization: A meta-analysis. Criminology*, v. 52, n.1, pp. 87–116, 2014.

RENGIER, Rudolf.*Strafrecht: Allgemeiner Teil*. 7. ed. Munique: Beck. 2012.

RICHARDSON, Ronny; NORTH, Max M. Ransomware: Evolution, mitigation and prevention. *International Management Review*, v. 13, n. 1, 2017.

RODOTÁ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014.

ROSSINI, Augusto. *Informática, telemática e Direito penal*. São Paulo: Memória Jurídica Editora, 2004.

ROXIN, Claus. *Derecho Penal: Parte General*. Madrid: Civitas, 1997.

ROXIN, Claus; GRECO, Luís. *Funcionalismo e Imputação Objetiva no Direito Penal*. trad. Luís Greco. Rio de Janeiro: Renovar, 2002.

ROXIN, Claus. *La teoría del delicto en la discusión actual*. Tradução de Manuel Abanto Vásquez. Lima: Grijley, 2007.

ROXIN, Claus. *Politica Criminal y estrutura del delito.* Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992.

SALDANHA, João. *Fundamentos da LGPD: a autodeterminação informativa*. 2019. Disponível em: https://triplait.com/a-autodeterminacao-informativa/. Acesso em: 17 dez. 2021.

SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro. In: De Lima, Cíntia Rosa Pereira (coord). *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020.

SARLET, Ingo Wolfgang. *Dignidade da Pessoa Humana e Direitos Fundamentais na Constiuição Federal de 1988*. 2. ed. Porto Alegre: Livraria do Advogado, 2002.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 7. ed. São Paulo: Saraiva, 2018.

SARRABAYROUSE, Facundo. Imputación objetiva, fraude inmobiliario y delito de estelionato. In: YACOBUCCI, Guillermo Jorge. *Derecho penal empresario*. Coordenação de Mario H. LAPORTA, Nicolás D. RAMÍREZ. Montevidéu: B. de F., 2010.

SCHELL, Bernadette Hlubik; SCHELL, Bernadette; MARTIN, Clemens. *Webster's new world hacker dictionary*. John Wiley & Sons, 2006.

SCHULTZ, Hans. *Kriminologische und strafrechtliche Bermekungen zur Beziehung zwischen Täter und Opfer.* ZStrR, v. 71, pp. 171-192, 1956.

SCHÜNEMANN, Bernd. As bases do processo penal transnacional. *Revista Brasileira de Ciências Criminais.* São Paulo, v. 19, n. 90, pp. 189-209, mai/jun. 2011.

SCHÜNEMANN, Bernd. Die kritik am strafrechtlichen paternalismus - eine sisyphus-arbeit?. *In: PATERNALISMUS im Strafrecht*: Die Kriminalisierung von selbstschädigendem Verhalten. Organização de Ulfrid NEUMANN, Kurt SEELMANN. Baden-Baden: Nomos, p. 221-240, 2010. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=83488. Acesso em: 5 out. 2020.

SCHÜNEMANN, Bernd. La relación entre ontologismo y normativismo em la dogmática jurídico-penal. *In:* CONGRESO INTERNACIONAL. FACULTAD DE DERECHO DE LA UNED. *Modernas tendencias em la ciencia del derecho penal y em la criminología.* Madrid: Universidad Nacional de Educación a Distancia, 2001.

SCHÜNEMANN, Bernd. El sistema del ilícito jurídico-penal: concepto de bien jurídico y victimodogmática como enlace entre el sistema de la parte general y de la parte especial. In: HERNÁNDEZ, Moisés Moreno (Coord.). *Problemas capitales del moderno derecho penal a principios del siglo XXI*, Editorial Ius Poenale, México D.F., pp. 87-113, 2003.

SCHÜNEMANN, Bernd. O direito penal é a ultima ratio da proteção de bens jurídicos: sobre os limites invioláveis do direito penal em um estado de direito liberal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 13, n. 53, p. 9-37, mar./abr. 2005. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=50732. Acesso em: 5 out. 2020.

SHECAIRA, Sergio Salomão. *Criminologia*. 6. ed. São Paulo: Revista dos Tribunais, 2014.

SIEBER, Ulrich. Computer Crime and Criminal Information Law: New Trends in the International Risk and Information Society. *COMCRIME Study*. European Commission, 1998. Disponível em: https://www.law.tuwien.ac.at/sieber.pdf. Acesso em 28 set. 2021.

SILVA SÁNCHEZ, Jesús María. Innovaciones teórico-prácticas de la Victimología en el Derecho penal. In: *Victimología: VIII Cursos de Verano en San Sebastián= VIII Udako Ikastaroak Donostian.* Universidad del País Vasco/Euskal Herriko Unibertsitatea, pp. 75-83, 1990.

SILVA SÁNCHEZ, José María. La consideración del comportamiento de la víctima en la teoria del delito: oservaciones doctrinales y jurisprudenciales sobre la "víctimo-dogmática". *RBCCRIM*, São Paulo, v 34, pp. 163-194, 2001.

SILVA SÁNCHEZ, Jesús-María; MORÁN, Ángel José Sanz. *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales.* Madrid: Civitas, 2001.

SILVA SÁNCHEZ, Jesús María. La víctima en el futuro de la dogmática. *Victimología*. San Sebastián: Universidad del País Vasco/Euskal Herriko Unibertsitatea, 1990.

SILVA SÁNCHEZ, Jesús María. Politica criminal en la dogmática: algunas cuestiones sobre su contenido y límites. In: *Política criminal y nuevo derecho penal: Libro homenaje a Claus Roxin*. Barcelona: Bosch, pp. 17-30, 1997.

SILVEIRA, Renato de Mello Jorge. *Fundamentos da adequação social em direito penal*. São Paulo: Quartier Latin, 2010.

SILVEIRA, Renato de Mello Jorge. *Direito Penal Supraindividual. Interesses difusos.* São Paulo: Revista dos Tribunais, 2003.

SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 2. ed. Salvador: Juspodivm, 2021.

SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.* Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009.

SYDOW, Spencer Toth. O bem jurídico nos crimes informáticos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 113, pp. 193-212, mar./abr. 2015. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=117946. Acesso em: 15 ago. 2020.

SOUZA, Luciano Anderson de. *Direito Penal*. v 1. São Paulo: Revista dos Tribunais, 2019.

TANGERINO, Dayane Aparecida Fanti. A (in)aplicabilidade da tese da autocolocação da vítima em risco aos delitos perpetrados por meio das novas tecnologias. *In: ESTUDOS em homenagem a Vicente Greco Filho*. Organização de Renato de Mello Jorge SILVEIRA, João Daniel RASSI. São Paulo: LiberArs, 2014. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=111521. Acesso em: 13 set. 2020.

TIEDEMANN, Klaus. *Poder económico y delito*. Tradução: Amelia Mantilla Villegas. Barcelona: Ariel, 1985.

VAN WILSEM, J. Bought it, but never got it: Assessing risk factors for online consumer fraud victimization**.** *European Sociological Review*, v. 29, pp. 168–178, 2013.

VIANNA, Túlio Lima. Do delito de dano e sua aplicação ao direito penal informático. *Revista de derecho informático*, n. 62, set. 2003.

VIANNA, Túlio; MACHADO, Felipe. *Crimes Informáticos: conforme a Lei n. 12.737/2012*. Belo Horizonte: Fórum, 2013.

WALL, D. S. Catching cybercriminals: Policing the Internet. *International Review of Law - Computers & Technology*, v. 12, pp. 201–218, 1998.

WILLEMS, Eddy. *Cyberdanger: Understanding and Guarding Against Cybercrime*. Springer, 2019.

WORTLEY, Richard; TOWNSLEY, Michael.Environmental criminology and crime analysis: Situating the theory, analytic approach and application. In: WORTLEY, R. ; TOWNSLEY, M. (eds). *Environmental Criminology and Crime Analysis*, 2. ed. London: Routledge, 2016.

XIE, Huagang; WANG, Xinran; LIU, Jiangxia. *Malware analysis system*. U.S. Patent n. 9,047,441, Publicação: 02 mai. 2011, Concessão: 02 jun. 2015, disponível em: https://patents.google.com/patent/US9047441B2/en. Acesso em: 29 set. 2021.

YAR, Majid. *Cybercrime and Society*. 2. ed, London: SAGE, 2013.

ZACZYK, Rainer. *Strafrechtliches Unrecht und die Selbstverantwortung des Verletzten***.** Heidelberg: Müller, 1993.

ZARGAR, Saman Taghavi; JOSHI, James; TIPPER, David. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, v. 15, n. 4, pp. 2046-2069, 2013.

Julgados

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação Cível n. 1012542-19.2021.8.26.0577, 23ª Câmara de Direito Privado, relator Hélio Nogueira, julgado em 20 out. 2021.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação Cível n. 1054914-30.2019.8.26.0002, 11ª Câmara de Direito Privado, Relator. Marco Fábio Morsello, julgado em 27 jul. 2020.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação Cível n. 1003235-49.2019.8.26.0597, 14ª Câmara de Direito Privado, Relator Thiago de Siqueira, julgado em 12 dez. 2019.